

**ФЕДЕРАЛЬНОЕ АГЕНСТВО СВЯЗИ  
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  
«САНКТ-ПЕТЕРБУРГСКИЙ  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ  
им. проф. М.А. БОНЧ-БРУЕВИЧА**

Лисица Вера Константиновна

Тестовые сценарии подсистемы ТСАР

Стека протоколов ОКС №7

Научный руководитель –  
доктор технических наук, профессор,  
Гольдштейн Борис Соломонович

Санкт-Петербург – 2007

## Список сокращений

АМТС	Автоматическая междугородная телефонная станция
АТС	Автоматическая телефонная станция
МСЭ	Международный союз электросвязи
ОКС	Общеканальная система сигнализации
СМО	Система массового обслуживания
СПС	Сети подвижной связи
ТфОП	Телефонная сеть общего пользования
УСС	Узел спецслужб
ЧНН	Час наибольшей нагрузки
ЭМВОС	Эталонная модель взаимосвязи открытых систем
AC	Authentication Center (центр аутентификации)
BS	Base Station (базовая станция)
BSC	Base Station Controller (контроллер базовых станций)
CPT	Compatibility Tests (тесты совместимости)
CSL	Component Sublayer (подуровень компонентов)
EIR	Equipment Identity Register (регистр идентификации оборудования)
EOC	End-of-Contents (конец содержания)
FISU	Full-in Signal Unit (заполняющая сигнальная единица)
GMSC	Gateway Mobile Switching Center (шлюзовый коммутационный центр подвижной связи)
GSM	Global System for Mobile Communications (общий цифровой стандарт мобильной связи)
GT	Global Title (глобальный адрес)
HLR	Home Location Register (домашний регистр местоположения)
HUP	Handover User Part (подсистема пользователей процедуры передачи управления в процессе разговора сети мобильной связи)
ID	Identifier (идентификатор)

IMSI	International Mobile Subscriber Identifier (международный идентификатор мобильного абонента)
INAP	Intelligent Network Application Part (прикладная подсистема пользователя интеллектуальной сети)
IP	Intelligent Peripheral (интеллектуальная периферия)
ISDN	Integrated Services Digital Network (цифровая сеть с интеграцией служб)
ISP	Intermediate Service Part (подсистема промежуточного обслуживания)
ISUP	Integrated Service User Part (подсистема пользователя ISDN)
LSSU	Link Status Signal Unit (сигнальная единица состояния звена)
MAP	Mobile Application Part (прикладная подсистема пользователя мобильной связи стандарта GSM)
MSC	Mobile Switching Center (коммутационный центр подвижной связи)
MSC	Message Sequence Chart (карты последовательностей сообщений)
MSISDN	Mobile Station ISDN number (ISDN-номер мобильной станции)
MSRN	Mobile Station Roaming Number (временный роуминговый номер)
MSU	Message Signal Unit (значащая сигнальная единица)
MTP	Message Transfer Part (подсистема переноса сообщений)
MUP	Mobile User Part (подсистема пользователя мобильной связи стандарта NMT-450)
NGN	Next Generation Network (сеть следующего поколения)
NMT	Nordic Mobile Telephone System (северный стандарт мобильной связи)
NSP	Network Service Part (подсистема сетевых услуг)
OMAP	Operations, Maintenance and Administration Part (прикладная подсистема эксплуатации, технического обслуживания и административного управления)
SCCP	Signalling Connection Control Part (подсистема управления соединением сигнализации)

SCEP	Service Creation Environment Point (центр программирования услуг)
SCP	Service Control Point (узел управления услугами)
SDL	Specification and Description Language (язык описания и детализации)
SDP	Service Data Point (блок данных услуг)
SEP	Signalling End Point (оконечный пункт сигнализации)
SIO	Service Information Octet (байт служебной информации)
SL	Signalling Link (сигнальное звено)
SMP	Service Managment Point (центр администрирования услуг)
SNT	Signalling Network Testing (протокол-тестер)
SP	Signalling Point (пункт сигнализации)
SPC	Signalling Point Code (код пункта сигнализации)
SSP	Service Switching Point (узел коммутации услуг)
STP	Signalling Transfer Point (транзитный пункт сигнализации)
TCAP	Transaction Capability Application Part (прикладная подсистема средств транзакции)
TSL	Transaction Sublayer (подуровень транзакции)
TUP	Telephone User Part (подсистема пользователя ТфОП)
VAT	Validation Test (тесты соответствия)
VLR	Visitor Location Register (гостевой регистр местоположения)

## Оглавление

Список сокращений.....	2
Введение.....	6
Глава 1. Система сигнализации ОКС №7 .....	8
1.1. Назначение и принцип функционирования ОКС №7.....	8
1.2. Архитектура системы ОКС №7.....	10
Глава 2. Подсистема TCAP.....	15
2.1. Назначение и архитектура подсистемы TCAP .....	15
2.2. Компоненты и примитивы TCAP .....	17
2.3. Структура сообщения TCAP .....	23
2.4. Пользователи TCAP .....	32
Глава 3. Тестирование протокола TCAP.....	38
3.1. Тестовая спецификация протокола TCAP .....	38
3.2. Язык MSC.....	41
3.3. Тестовая платформа SNT.....	43
Глава 4. Разработка тестовых сценариев TCAP .....	48
4.1. Тестовые сценарии для услуги «800».....	48
4.2. Тестовые сценарии для услуги «телеголосование» .....	52
4.3. Тестовые сценарии для услуги «роуминг» .....	56
4.4. Анализ временных характеристик сообщений TCAP .....	63
Заключение.....	73
Список литературы .....	74
<i>Приложение 1</i> .....	76
<i>Приложение 2</i> .....	77
<i>Приложение 3</i> .....	78

## Введение

По мере развития телекоммуникационных систем возрастает значимость систем сигнализации, назначением которых является обеспечение взаимодействия различных сетевых устройств. В виду многообразия современных сетей связи и их структурного усложнения, актуальными становятся такие требования к системам сигнализации, как универсальность, эффективность и высокая надежность передачи информации. Система ОКС №7 на сегодняшний день является единственной системой сигнализации, удовлетворяющей этим требованиям. Эта система стандартизована для применения как на международных, так и на национальных сетях связи и разработана в соответствии с эталонной моделью взаимосвязи открытых систем. Система ОКС №7 имеет многоуровневую структуру и состоит из подсистемы переноса сообщений и подсистем-пользователей.

Подсистема ТСАР относится к числу подсистем-пользователей стека ОКС №7. Подсистема ТСАР использует нижележащие подсистемы (МТР, SССР) для передачи своих сообщений по сети. В свою очередь ТСАР предоставляет свои услуги вышележащим уровням (IНАР, МАР, ОМАР). Подсистема ТСАР не предоставляет каких-либо услуг пользователю непосредственно, но ее возможности для предоставления своих услуг используют, например, интеллектуальная сеть и сеть подвижной связи. В самом деле, сегодня, когда спрос пользователя постоянно возрастает не только на услуги коммутации, но и на специальные услуги, важность применения подсистемы ТСАР неоспорима. Несмотря на это, подсистема ТСАР недостаточно освещена в российской литературе. Одной из задач автора является описание подсистемы ТСАР.

При проектировании любых сетей связи, и в частности с ТСАР, важным этапом является тестирование программно-аппаратных средств реализации протоколов. В связи с этим чрезвычайно важно наличие эффективных программно-аппаратных средств тестирования протокольных реализаций систем сигнализации. Как правило, такие средства тестирования содержат набор тестов-

вых сценариев, в соответствии с которыми происходит отладка той или иной системы.

В соответствии со сказанным выше, становится понятна необходимость создания сценариев тестирования для подсистемы ТСАР.

Также при проектировании сети с ТСАР необходимо учесть временные задержки сообщений ТСАР, которые возникают в процессе осуществления диалога ТСАР при взаимодействии элементов сети, поскольку они могут оказать существенное влияние на качество предоставляемых услуг. Поэтому представление модели расчета временных задержек сообщений ТСАР, с помощью которой можно было бы в дальнейшем в соответствии со статистическими данными определить их значения для каждого конкретного случая, является необходимой частью данного исследования.

Решению всех этих актуальных проблем и посвящена данная работа.

Целью исследования является разработка тестовых сценариев подсистемы ТСАР стека протоколов ОКС №7, что предполагает постановку и решение следующих задач:

1. Рассмотрение архитектуры системы сигнализации ОКС №7 и принципов ее функционирования.
2. Описание назначения и архитектуры подсистемы ТСАР и принципов ее функционирования.
3. Изучение принципов тестирования подсистемы ТСАР.
4. Разработка и описание тестовых сценариев подсистемы ТСАР для некоторых услуг, предоставляемых интеллектуальной сетью и сетью подвижной связи.
5. Расчет временных задержек сообщений ТСАР.

Содержание работы изложено на 75 страницах, включая 1 таблицу, 20 рисунков, и состоит из введения, четырех глав, заключения, библиографического списка из 16 наименований и 3-х приложений.

## **Глава 1. Система сигнализации ОКС №7**

### **1.1. Назначение и принцип функционирования ОКС №7**

В ходе исторического развития классических телефонных сетей были разработаны различные международные и национальные варианты телефонных систем сигнализации, обеспечивающие передачу сигналов управления и взаимодействия между сетевыми узлами в процессе обслуживания вызовов. В последнее время на базе ресурсов телефонных сетей или при взаимодействии с ними реализуются такие новые сетевые технологии, как цифровые сети с интеграцией обслуживания, сотовые сети подвижной связи, интеллектуальные сети. Для реализации соответствующих услуг в этих сетях требуется быстрая и надежная передача большого объема данных между узлами. Реализовать это средствами телефонной сигнализации не представляется возможным. [8]

В этих условиях одним из главных направлений в развитии современных сетей связи является применение общеканальной системы сигнализации №7, стандартизованной для применения как на международных, так и на национальных сетях связи. Разработанная в соответствии с эталонной моделью взаимосвязи открытых систем, система ОКС №7 является в настоящее время единственной универсальной системой сигнализации, обеспечивающей эффективное функционирование современных и перспективных сетей телекоммуникаций. [8]

Система ОКС №7 – это такая система сигнализации, при которой информация управления установлением соединения для всех разговорных каналов и/или каналов передачи данных передается в виде блоков данных (сигнальных сообщений) по одному общему каналу сигнализации, который может быть организован в любом временном интервале (кроме нулевого) одного из первичных трактов ИКМ, входящих в пучок, соединяющий напрямую две взаимодействующие АТС. Как правило, для повышения надежности в другом ИКМ-

тракте пучка, организуется резервный канал для передачи данных ОКС №7. Система ОКС №7, по сути, является специализированной системой передачи данных с коммутацией пакетов, работающей по цифровым каналам со скоростью 64 кбит/с. [4, 8]

Сеть связи, использующая ОКС №7, состоит из множества узлов коммутации, связанных между собой цифровыми ИКМ-трактами. Чтобы имелась возможность при управлении соединениями пользоваться услугами ОКС №7, каждый из этих узлов должен содержать встроенный программно-аппаратный модуль – сигнальный терминал – благодаря которому он мог бы выполнять функции пункта сигнализации (SP), способного формировать, передавать и интерпретировать сигнальные сообщения. Пункты сигнализации могут быть оконечными (SEP) и транзитными (STP). Транзитные пункты сигнализации, в отличие от оконечных, переносят принятые сообщения из входящего сигнального звена в исходящее, не направляя при этом сигнальное сообщение на обработку к подсистеме-пользователю. Каждому пункту сигнализации в сети ОКС №7 назначается уникальный номер – код пункта сигнализации (SPC). [4]

Пункты сигнализации должны быть связаны между собой цифровыми двунаправленными каналами, используемыми в качестве среды передачи сигнальной информации и называемыми звеньями передачи данных. Звено передачи данных и сигнальный терминал в совокупности составляют сигнальное звено (SL). Одно или несколько сигнальных звеньев между двумя соединенными напрямую пунктами сигнализации образуют пучок сигнальных звеньев, причем совокупность сигнальных звеньев в одном пучке, имеющих идентичные характеристики, называется группой сигнальных звеньев. [4]

Таким образом, сеть общеканальной сигнализации – это совокупность пунктов сигнализации и соединяющих их сигнальных звеньев. Для построения сети ОКС №7, как правило, используются два варианта: квазисвязанный и связанный. Сеть называется квазисвязанной, если ее топология не совпадает с базовой (телефонной) сетью. Соответственно сеть ОКС №7 называется связанной в противном случае. [1, 4]

## 1.2. Архитектура системы ОКС №7

Архитектура системы ОКС №7 устроена так, что множество всех функций системы представлено в виде совокупности функциональных блоков (именуемых подсистемами), определенным образом взаимодействующих между собой и поддерживающих друг друга [4].

Система сигнализации ОКС №7 построена по принципам, определенной эталонной моделью взаимосвязи открытых систем. Однако уровни модели ОКС №7 не полностью совпадают с уровнями ЭМВОС. В то время как ЭМВОС содержит семь уровней, модель ОКС №7 содержит только четыре уровня. Функции, выполняемые этими четырьмя уровнями, определенным образом соотносятся с функциями семи уровней ЭМВОС. При этом некоторые из уровней, входящих в модель взаимосвязи открытых систем, не имеют смысла в модели ОКС №7 и поэтому в ней не определены. Сопоставление двух моделей приведено на рис. 1.1. [4]

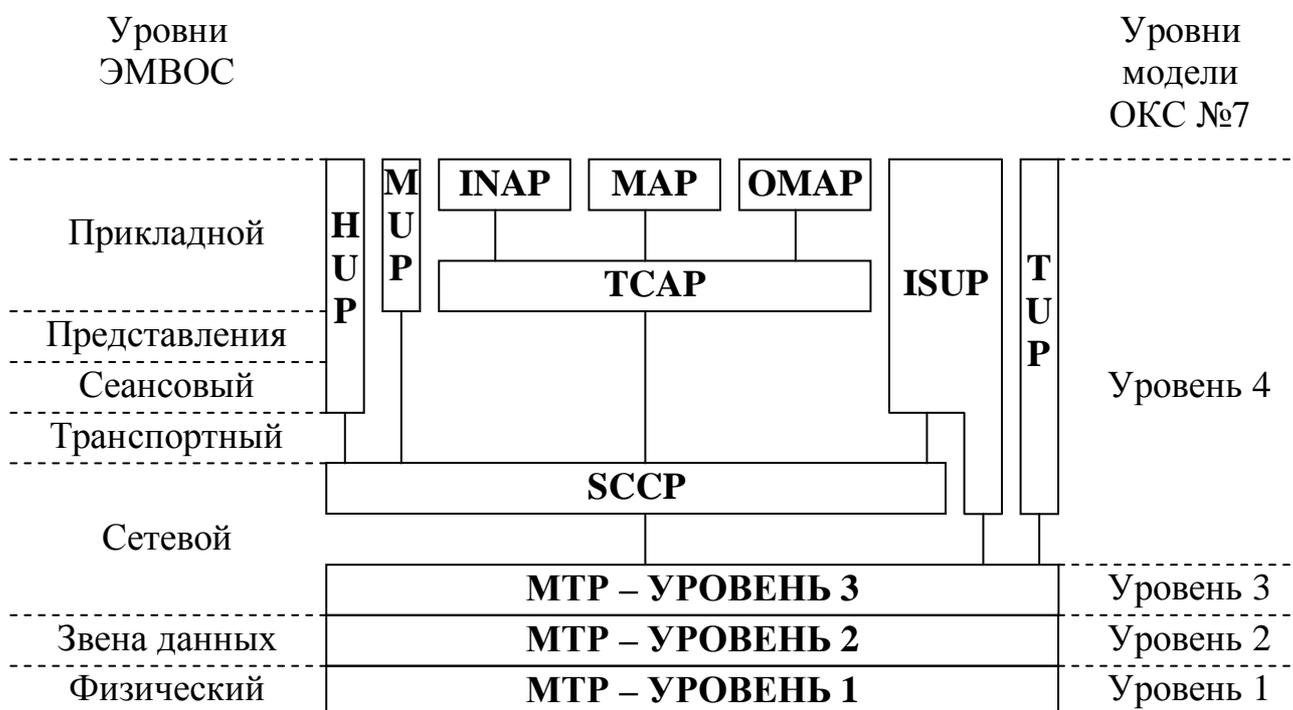


Рис. 1.1. Сопоставление уровней ЭМВОС и модели ОКС №7.

Три нижних уровня модели ОКС №7 образуют подсистему переноса сообщений МТР [4].

Уровень 1 – функции звена передачи данных – определяет физические, электрические и функциональные характеристики канала передачи данных для звена. Более высокие уровни не зависят от принятой системы передачи. [2]

Уровень 2 – функции сигнального звена – определяет функции и процедуры, относящиеся к передаче сигнальных сообщений по сигнальному звену. Сигнальное сообщение, поступающее от верхних уровней, проходит по сигнальному звену в виде сигнальных единиц переменной длины. Функциями сигнального звена являются деление сигнальных сообщений на сигнальные единицы, обнаружение и исправление ошибок в сигнальных единицах и т.д. [2, 8]

Уровень 3 – сетевые функции – определяет функции и процедуры передачи, общие для различных типов сигнальных звеньев и независимые от работы каждого из них. Процедуры уровня 3 обеспечивают надежную передачу сигнальной информации от одной АТС к другой даже в случае отказов на уровнях 1 и 2. Уровень 3 обеспечивает управление сигнальными звеньями и включает функции обработки сигнальных сообщений для их маршрутизации в сети сигнализации, а также функции управления самой сетью сигнализации. [2, 8]

Таким образом, подсистема МТР является единой транспортной платформой, над которой расположены подсистемы пользователей, предназначенные для обеспечения соответствующих услуг связи. Эта подсистема предоставляет транспортную услугу без установления соединения, но с упорядоченной последовательностью передачи. Подсистема МТР обеспечивает передачу информации в неискаженной форме, без потерь, дублирования ошибок, в установленной последовательности от одного пункта сигнализации к другому. [6]

Уровень 4 – функции подсистем пользователей – состоит из различных подсистем пользователей, каждая из которых определяет функции и процедуры сигнализации, характерные для определенного типа пользователя системы. Набор функций подсистемы пользователя может значительно различаться для разных категорий пользователей системы сигнализации. [8]

Основными подсистемами пользователей ОКС №7 являются:

- подсистема управления соединением сигнализации (SCCP), дополняющая функциональные возможности подсистемы МТР и предоставляющая услуги сети, ориентированные или не ориентированные на установление соединения для передачи сигнальной информации, относящейся или не относящейся к разговорным каналам;
- подсистема пользователя ISDN (ISUP), обеспечивающая поддержку всех дополнительных видов обслуживания ISDN в цифровой сети и основного телефонного соединения;
- подсистема пользователя ТфОП (TUP), обеспечивающая необходимые функции и процедуры системы сигнализации ОКС №7 в телефонной сети;
- прикладная подсистема средств транзакции (TCAP), обеспечивающая (совместно с SCCP и МТР) передачу через сеть информации, не относящейся к разговорному каналу;
- прикладная подсистема пользователя интеллектуальной сети (INAP), обеспечивающая необходимые функции и процедуры системы сигнализации ОКС №7 в интеллектуальной сети;
- прикладная подсистема пользователя мобильной связи стандарта GSM (MAP), обеспечивающая необходимые функции и процедуры системы сигнализации ОКС №7 в сотовой сети стандарта GSM;
- подсистема пользователя мобильной связи стандарта NMT-450 (MUP), обеспечивающая связь при передвижении абонентов между центрами коммутации сотовых сетей связи стандарта NMT-450, т.е. для обеспечения роуминга;
- подсистема пользователей процедуры передачи управления в процессе разговора сети мобильной связи (HUP), предназначенная для сигнализации при передаче соединения (хенд-овер) между обслуживающими вызов телефонными станциями подвижной связи стандарта NMT-450, непосредственно соединенными прямыми телефонными каналами для передачи речи;
- прикладная подсистема эксплуатации, технического обслуживания и административного управления (OMAP), обеспечивающая необходимые функции

и процедуры системы сигнализации ОКС №7 в сети управления и техэксплуатации. [2, 8]

Два первых уровня модели ОКС №7 обеспечивают обмен сигнальной информацией между двумя смежными пунктами сигнализации, и их функции полностью совпадают с функциями физического уровня и уровня звена данных ЭМВОС. Однако реализованный в подсистеме МТР третий, сетевой уровень, содержит не все функции сетевого уровня модели ЭМВОС. Для поддержки новых услуг (в том числе, услуг интеллектуальной сети и мобильной связи) и для реализации недостающих функций сетевого уровня в модель ОКС №7 введена подсистема управления сигнальными соединениями SCCP. Подсистемы МТР и SCCP совместно образуют подсистему сетевых услуг (NSP). Используя услуги МТР, подсистема SCCP обеспечивает организацию в сети ОКС №7 виртуальных соединений и может предоставлять сетевые услуги, как ориентированные на такие соединения, так и не требующие их создания. [4]

Возможности МТР в области адресации являются ограниченными, так как эта подсистема может направлять сообщения только в те логические точки пункта сигнализации, адреса которых указаны в четырехбитовом поле индикатора службы октета SIO. Таким образом, в пределах конкретного пункта сигнализации МТР имеет возможность распределять сообщения к любому из максимум 16 пользователей, что явно недостаточно. Подсистема SCCP имеет расширенные возможности, рассматривая всех своих локальных пользователей как подсистемы (обращение к которым происходит путем использования их номеров) и применяя при адресации сообщений совокупность кода пункта назначения с номером подсистемы. Для идентификации конкретного адреса может обеспечиваться вычисление кода пункта сигнализации и номера подсистемы из так называемого глобального адреса (GT). Глобальный адрес может содержать телефонный или ISDN-номер, номер терминала сети передачи данных или номер любой другой специализированной сети. [4]

В дополнение к расширенным возможностям адресации подсистема SCCP предоставляет четыре различные по надежности класса обслуживания

(режима доставки сообщений), которые могут быть затребованы вышестоящей подсистемой [4].

В системе ОКС №7 пока не специфицированы подсистемы, предоставляющие услуги, ориентированные на установление соединений, вследствие чего транспортный, сеансовый уровни и уровень представления данных в том виде, в каком они определены в ЭМВОС, в модели ОКС №7 отсутствуют [4].

Выводы по главе. Таким образом, можно сказать, что на сегодняшний день система ОКС №7 является наиболее универсальной и эффективной системой сигнализации, которая находит применения в различных сетях связи. Система ОКС №7 разработана с учетом ее согласования с ЭМВОС. Она также имеет многоуровневую структуру, но ее уровни не идентичны уровням эталонной модели. Три нижних уровня ОКС №7 образуют подсистему МТР, которая отвечает за формирование и передачу сигнальных единиц по сети, и обеспечивают функции физического уровня, уровня звена данных и частично сетевого уровня ЭМВОС. Для выполнения всех функций сетевого уровня на четвертом уровне модели ОКС №7 добавлена подсистема SССР. Также на четвертом уровне определены функции и процедуры для различных подсистем пользователей, таких как ISUP, TUP, TСАР, INAP, MAP, MUP, HUP, OMAP. Основными элементами сети ОКС №7 являются пункты сигнализации и транзитные пункты сигнализации. Для построения сети ОКС №7, как правило, используются два варианта: квазисвязанный и связанный.

## Глава 2. Подсистема ТСАР

### 2.1. Назначение и архитектура подсистемы ТСАР

Прикладная подсистема средств транзакции (ТСАР) является прикладным протоколом системы ОКС №7, который используется множеством распределенных приложений и вместе с соответствующими услугами подсистем SССР и МТР обеспечивает передачу через сеть информации, не относящейся к каналу. В общем виде вариантами применения ТСАР являются ситуации, когда установление основного соединения наряду с сигнальным невозможно или не требуется. [2, 9]

Средства транзакций могут использоваться для поддержки обмена информацией между:

- станциями и/или узлами коммутации сети;
- станцией (узлом коммутации) и специализированным сетевым центром (базой данных, пунктом управления услугами интеллектуальной сети, центром технической эксплуатации и т.п.);
- специализированными сетевыми центрами. [2]

Следующие приложения являются пользователями ТСАР [8]:

- передача сообщений о местонахождении мобильного пользователя в регистр домашнего пользователя в сотовых сетях (для реализации роуминга);
- регистрация, активация и вызов дополнительных услуг, включая использование специализированного оборудования (например, при предоставлении услуг телефонного обслуживания по кредитной карточке в интеллектуальной сети);
- обмен сигнальной информацией, не связанной с коммутируемым информационным каналом (например, замкнутая группа пользователей, процедура перезаказа);

- процедуры техобслуживания и эксплуатации (например, управление удаленной станцией) и др.

Все такого рода приложения можно разделить на две категории [2, 8]:

- работающие в режиме реального времени, при этом услуги ТСАР (в дальнейшем называемые ТС-услугами) базируются на сетевых службах не ориентированных на соединение, в этом случае объем данных относительно невелик;
- не работающие в режиме реального времени, при этом ТС-услуги базируются на сетевых службах, ориентированных на соединение, в этом случае объем данных может быть очень большим.

Термин «средства транзакции» относится к услугам и протоколам уровня приложений (уровня 7 ЭМВОС), реализуемым в подсистеме ТСАР, а также к услугам и протоколам, выполняющим функции представления, поддержки сессии и транспортные функции (то есть функции уровней 6, 5 и 4 ЭМВОС) и реализуемым, когда это требуется, подсистемой промежуточного обслуживания (ISP). Подсистема ISP требуется только тогда, когда должны передаваться большие объемы данных, используя один из классов SCCP с установлением логического соединения. В настоящее время во всех известных применениях подсистема ТСАР предоставляет пользователям услуги, основанные на сетевой службе, не ориентированной на соединение. Для таких применений транспортный, сеансовый уровни и уровень представления ЭМВОС не нужны, следовательно, подсистема промежуточного обслуживания ISP не предоставляет никаких функций. В этом случае ТСАР осуществляет интерфейс напрямую с SCCP (рис 2.1). [8]

Архитектура подсистемы ТСАР состоит из двух подуровней: подуровня компонентов (CSL) и подуровня транзакции (TSL) (рис 2.1).

Подуровень компонентов обеспечивает прием и передачу запросов от пользователя и к пользователю услугами ТСАР (в дальнейшем называемых ТС-пользователями). Подуровень компонентов имеет дело с индивидуальными

действиями или данными, называемыми компонентами и выполняет две функции – обработку диалога и обработку компонентов. [8]

Подуровень транзакций обеспечивает возможность обмена компонентами между пользователями подуровня транзакции (в дальнейшем называемых TR-пользователями), а также использования услуг нижележащих уровней (подсистем SCCP и MTP) для двустороннего переноса через сеть ОКС сообщений между рабочими TR-единицами двух взаимодействующих подсистем TCAP, размещенных в разных пунктах этой сети. Единственным видимым на данный момент TR-пользователем является подуровень компонентов. [2, 8]



Рис. 2.1. Архитектура подсистемы TCAP и ее положение в ОКС №7.

## 2.2. Компоненты и примитивы TCAP

Обмен информацией между ТС-пользователями происходит посредством приема и передачи компонентов. Компонент представляет собой блок данных, содержащих запрос на выполнение какой либо операции или отклик на этот запрос. Компонент, связанный с вызовом определенной операции, снабжается идентификатором (ID вызова). Операция представляет собой действие, которое должно быть выполнено на удаленном конце. Только один отклик может

быть послан в ответ на данную операцию. Отклик, как правило, несет информацию об успешном или неуспешном выполнении операции. [2]

Существуют компоненты следующих пяти типов:

1. **INVOKE** (вызов операции). Этот компонент запрашивает выполнение встречной стороной определенной операции. Он может быть связан с другим запросом, ранее посланным встречной стороной. Каждый компонент содержит идентификатор вызова, чтобы можно было однозначно закрепить различные компоненты за операцией или диалогом. Компонент **INVOKE** также может содержать примыкающий идентификатор, позволяющий определить связь между разными диалогами. Примыкающий идентификатор содержит значение идентификатора вызова второго диалога, который связан с первым.
2. **RETURN RESULT NOT LAST** (часть данных с информацией о результате выполнении операции). Компонент **RETURN RESULT NOT LAST** является результатом диалога, открытого компонентом **INVOKE**. Заметим, что из-за ограниченной емкости сообщений передаваемые данные результата могут быть сегментированы. В этом случае для всех сегментов данных кроме самого последнего используется компонент **RETURN RESULT (NOT LAST)**.
3. **RETURN RESULT LAST** (последняя или единственная часть данных с информацией о результате выполнении операции). Этот компонент свидетельствует об успешном завершении операции. Он может содержать последний (или единственный) сегмент результата.
4. **RETURN ERROR** (возврат ошибки). Этот компонент информирует о том, что операция не была успешно завершена.
5. **REJECT** (отказ в приеме к обработке компонента, поступившего от встречной стороны). Компонент **REJECT** содержит информацию о вызвавшей его причине – либо отсутствие ресурсов, нужных для выполнения операции, либо наличие в поступившем компоненте той или иной ошибки (компонент неизвестного типа, компонент с нестандартной структурой или со структурой, не соответствующей объявленному типу компонента, компонент с недопустимым или с используемым для другой операции идентификатором

обращения, компонент с неизвестным кодом операции, компонент, содержащий параметр несоответствующего типа, и т. п.). [2, 9, 10]

Последовательность компонентов, которыми обмениваются между собой два ТС-пользователя при выполнении одного приложения, образует диалог. Как было сказано в предыдущем пункте, функции обработки компонентов и обработки диалога выполняет подуровень компонентов. [2, 12]

Подуровень компонентов обеспечивает диалог между пользователями подсистемы ТСАР в двух возможных вариантах: неструктурированный и структурированный диалог [1].

При неструктурированном диалоге ТС-пользователи посылают компоненты, которые не требуют подтверждения для формирования однозначной взаимосвязи между ними. Однозначная взаимосвязь всегда существует между соединенными ТС-пользователями. Если один ТС-пользователь посылает однонаправленное сообщение другому такому же участнику, то это говорит об использовании неструктурированного диалога. Любой ТС-пользователь может иметь произвольное количество активных операций в произвольный данный момент времени, максимальное число которых зависит от числа уникальных ID вызовов, доступных ему в любой момент времени. [8]

При структурированном диалоге ТС-пользователь указывает начало, продолжение и окончание диалога. Использование структурированного диалога позволяет двум ТС-пользователям вести одновременно несколько диалогов, каждый из которых идентифицируется особым идентификатором диалога (ID диалога). Каждый ID диалога имеет выделенное именованное пространство ID вызова, что позволяет дублировать ID вызовов в различных диалогах. Порядок доставки сообщений может быть обеспечен при помощи прикладных протоколов или при использовании соответствующего класса услуги. [8]

Структурированный диалог предполагается двусторонним – на фазе его продолжения возможен дуплексный обмен компонентами [2].

Подуровень компонентов обеспечивает взаимосвязь запросов и откликов. Все операции, запрашиваемые подуровнем компонентов, можно разделить

на четыре класса, в соответствии с уровнем ответа, ожидаемым по завершении операции [2, 8]:

- класс 1 – подтверждение как успешного, так и неуспешного завершения операции;
- класс 2 – сообщается только неуспешное завершение операции;
- класс 3 – сообщается только успешное завершение операции;
- класс 4 – не сообщается ни успешное, ни неуспешное завершение операции.

Функции формирования и передачи TR-сообщение, содержащего один или несколько компонентов выполняет подуровень транзакций. Последовательность TR-сообщений, которыми обмениваются между собой два TR-пользователя при выполнении одного приложения, образует диалог. Также как и подуровень компонентов, подуровень транзакций обеспечивает возможность организации структурированного и неструктурированного диалога. Неструктурированный диалог в этом случае предоставляет возможность послать удаленному TR-пользователю один или несколько компонентов, которые не ожидают ответа, сгруппированные в однонаправленное сообщение. Структурированный диалог позволяет TR-пользователю начать диалог, обменяться компонентами в этом диалоге, закончить или прервать его. [8]

Существуют пять типов сообщений подуровня транзакций:

1. UNIDIRECTIONAL (однонаправленное). Сообщения UNIDIRECTIONAL связаны с неструктурированным диалогом.
2. BEGIN (начало). Это сообщение используется для установления транзакции с удаленным одноранговым подуровнем транзакций. Сообщение BEGIN может включать один или более компонентов.
3. CONTINUE (продолжение). Сообщение CONTINUE следует за сообщением BEGIN для передачи дополнительной информации, связанной с транзакцией. Сообщение CONTINUE содержит один или более компонентов.
4. END (окончание). Сообщение END используется для завершения транзакции. Все остающиеся не переданные компоненты включены в сообщение END. Существует два метода благополучного окончания транзакции: базо-

вый и подготовительный. В случае применения базового метода оба TR-пользователя информируются об окончании транзакции. Подготовительный метод обычно используют, когда TR-пользователи заранее договариваются о том, что каждый из них может решить завершить транзакцию, не информируя об этом другого TR-пользователя, который примет подобное решение самостоятельно.

5. ABORT (непредвиденное прекращение). Сообщение ABORT используется для завершения транзакции в аварийной ситуации. [1, 9, 12]

Обмен информацией между ТС-пользователями и подсистемой ТСАР осуществляется посредством примитивов. Примитивом называется абстрактное представление элемента взаимодействия внутри одной системы между группой функций, предоставляющей свои услуги, и группой функций, пользующейся этими услугами. От ТС-пользователя поступают примитивы запроса, а от подсистемы ТСАР – примитивы индикации. [2, 8]

Для обработки компонентов на их подуровне используются следующие примитивы [1, 8, 2]:

1. ТС-INVOKE (ТС-ВЫЗОВ). Этот примитив определяет вызов операции, которая может быть связана с другой операцией по обработке компонентов.
2. ТС-RESULT-L (ТС-РЕЗУЛЬТАТ). Этот примитив определяет успешную операцию или последнюю успешную часть сегментированной процедуры по обработке компонент.
3. ТС-RESULT-NL (ТС-ПРОМЕЖУТОЧНЫЙ РЕЗУЛЬТАТ). Этот примитив определяет успешную операцию промежуточной части сегментированной процедуры по обработке компонент.
4. ТС-U-ERROR (ТС-П-ОШИБКА). Этот примитив определяет, что произошел отказ при выполнении операции.
5. ТС-L-CANCEL (ТС-М-ОТМЕНА). Этот примитив информирует ТС-пользователя, что вызов операции прекращен по причине перерасхода времени.

6. TC-U-CANCEL (ТС-П-ОТМЕНА). Этот примитив вызывает местное прекращение вызова операции вследствие решения ТС-пользователя.
7. TC-L-REJECT (ТС-М-ОТКЛОНЕНИЕ). Этот примитив информирует местного ТС-пользователя о выявлении подуровнем компонентов неправильно сформированного компонента.
8. TC-R-REJECT (ТС-У-ОТКЛОНЕНИЕ). Этот примитив информирует местного ТС-пользователя об отклонении компоненты подуровнем компонентов.
9. TC-U-REJECT (ТС-М-ОТКЛОНЕНИЕ). Этот примитив указывает на отклонение компонента со стороны ТС-пользователя.

Примитивы TC-INVOKE, TC-RESULT-L, TC-RESULT-NL, TC-U-ERROR, TC-U-CANCEL имеют два возможных варианта: «запрос» и «индикация». Примитивы TC-L-CANCEL, TC-L-REJECT, TC-R-REJECT имеют только форму «индикация», а примитив TC-U-REJECT – форму «запрос». [1]

Подуровень компонент включает следующие примитивы для поддержки диалога [1, 2, 8]:

1. TC-UNI (ТС-ОДНОНАПРАВЛЕННОСТЬ). Этот примитив определяет неструктурированный диалог.
2. TC-BEGIN (ТС-НАЧАЛО). Этот примитив определяет начало структурированного диалога.
3. TC-CONTINUE (ТС-ПРОДОЛЖЕНИЕ). Этот примитив определяет продолжение для структурированного диалога.
4. TC-END (ТС-ОКОНЧАНИЕ). Этот примитив определяет конец структурированного диалога.
5. TC-U-ABORT (ТС-П-СБРОС). Этот примитив позволяет ТС-пользователю внезапно прекратить диалог без передачи каких-либо компонентов в продолжение.
6. TC-P-ABORT (ТС-С-СБРОС). Этот примитив сообщает ТС-пользователю о том, что диалог был прекращен поставщиком службы в ответ на прекращение транзакции.

Примитивы TC-UNI, TC-BEGIN, TC-CONTINUE, TC-END, TC-U-ABORT имеют два возможных варианта: «запрос» и «индикация». Примитив TC-P-ABORT имеет только форму «индикация». [1]

Подуровень транзакций включает следующие примитивы [1, 2, 8]:

1. TR-UNI (TR-ОДНОНАПРАВЛЕННОСТЬ). Этот примитив определяет неструктурированный диалог.
2. TR-BEGIN (TR-НАЧАЛО). Этот примитив определяет начало структурированного диалога.
3. TR-CONTINUE (TR-ПРОДОЛЖЕНИЕ). Этот примитив определяет продолжение для структурированного диалога.
4. TR-END (TR-ОКОНЧАНИЕ). Этот примитив определяет конец структурированного диалога.
5. TR-U-ABORT (TR-П-СБРОС). Этот примитив позволяет TR-пользователю внезапно прекратить диалог без передачи каких-либо компонентов в продолжение.
6. TR-P-ABORT (TR-С-СБРОС). Этот примитив сообщает TR-пользователю о том, что диалог был прекращен поставщиком службы в ответ на прекращение транзакции.

Примитивы TR-UNI, TR-BEGIN, TR-CONTINUE, TR-END, TR-U-ABORT имеют два возможных варианта: «запрос» и «индикация». Примитив TR-P-ABORT имеет только форму «индикация». [1]

### **2.3. Структура сообщения TCAP**

Любое сообщение TCAP состоит из некоторого количества информационных элементов, размещенных в нем по определенным правилам. В информационном элементе имеется три поля, содержащих каждое целое число байтов и расположенных в следующей последовательности [2, 8]:

- Тег;
- Длина;
- Содержание.

Поле «тег» является первым полем информационного элемента ТСАР, отличает один элемент информации от другого и управляет интерпретацией информации, заключенной в поле «содержание». Это поле состоит из трех частей: «класс», «форма» и «код тега». Заметим, что указанные длины и информация о битах на рис. 2.2. относятся только к полю «тег» длиной 1 байт. [8, 10]

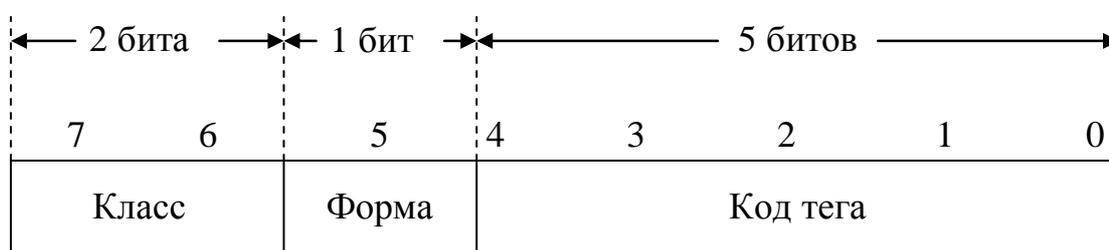


Рис. 2.2. Формат поля «тег» длиной 1 байт.

Поле «класс» определяет тип данных. Нужно различать четыре класса, список которых приведен в таблице 2.1.

Таблица 2.1

#### Классы тегов

Класс тега	Кодировка битов
Универсальный	00
Прикладной	01
Контекстно зависимый	10
Применение пользователя	11

Универсальный тип используется для ярлыков, которые особо стандартизированы в рекомендациях. Универсальные ярлыки могут использоваться в любом месте, где используется универсальный элемент информации. [8]

Прикладной тип используется для элементов информации, которые стандартизированы для всех приложений, использующих средства транзакции ОКС №7, т.е. ТС-пользователей [8].

Тип «контекстно зависимый» используется для элементов информации, которые определены в контексте последующей более высокой конструкции и

зависят от порядка других элементов данных в этой конструкции. Этот тип может использоваться для создания ярлыка составного элемента. [8]

Тип «применение пользователя» используется для данных специального типа, которые не определены в рекомендациях (данные сетевого оператора или провайдера услуг) [10].

Поле «форма» используется для обозначения формы представления элемента. Если поле «форма» имеет значение «0», то это значит, что поле данных содержит простой элемент, т.е. параметр больше не разбивается на части. Если поле «форма» имеет значение «1», то это значит, что поле данных содержит составной элемент; в этом случае поле «тег» является только групповой ссылкой для параметров в последующем поле данных. [8, 10]

Поле «код тега» указывает получателю сообщения, какой тип параметров содержит поле данных. Поле «код тега» содержит пять битов. В некоторых приложениях этого может не хватать. Решение проблемы состоит в расширении поля «тег» до необходимой длины. Чтобы выполнить это расширение используется специальный метод, который иллюстрируется на рис. 2.3. [10]

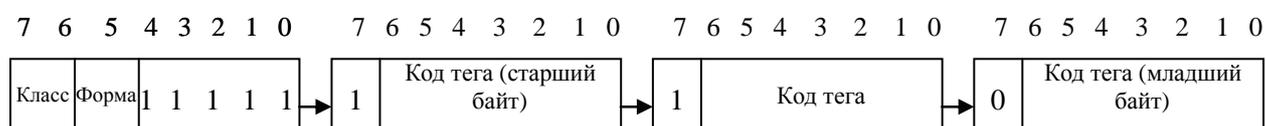


Рис. 2.3. Формат поля «тег» длиной более 1 байта.

Поле «тег» длиной 1 байт используется для всех значений типов параметров, меньших 31. При этом максимальное значения поля «Код» представляется следующим образом – 11110 (рис. 2.2). [10]

Если значение типа параметров превышает 30, то для того, чтобы закодировать такую величину необходимо более одного октета (рис. 2.3). Поэтому значение 11111 для первого байта поля «тег» зарезервировано в качестве указателя расширения. При таком способе кодирования биты с 0 по 6 следующих октетов содержат фактическое значение типа параметров, а бит 7 всегда указывает, следует ли далее другой октет с полем «код тега». Если бит 7 установлен в 1, следующий октет тоже содержит информацию тега; если бит 7 установлен в

0, тег заканчивается этим октетом. Бит 6 второго октета является старшим значащим битом, в то время как бит 0 последнего октета представляет собой младший значащий бит. [10]

При кодировании длины содержания возникают проблемы, аналогичные тем, которые описаны для кодирования тега. Теоретический предел для кодирования поля длины с использованием только одного байта равен 255 байтов. В данное время для всех практических целей этого количества было бы достаточно, поскольку сообщения SCCP ограничены 255 байтами. Однако, чтобы застраховаться на будущее и обеспечить возможность внедрения дополнительных приложений, необходимо выработать решение, которое позволит кодировать поле любой необходимой длины. [10]

Длина содержания имеет короткую, длинную или неопределенную форму представления [8].

Если длина менее 128 байтов (рис. 2.4), используется короткая форма, при этом поле указателя длины имеет длину 1 байт. Используются только биты с 0 по 6, что позволяет кодировать значения между 0 и 127 (01111111). Бит 7 всегда равен 0, следовательно, предел в 255 байтов длины достигнуть невозможно. [8, 10]

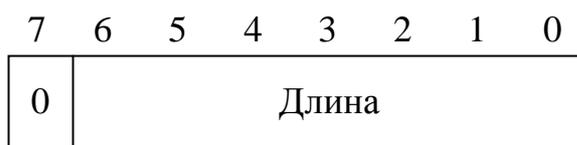


Рис. 2.4. Короткая форма представления поля «длина».

Если длина более 127 байтов (рис. 2.5), используется длинная форма представления, при поле указателя длины необходимо расширить на достаточное количество байтов. Для этой цели бит 7 устанавливается в 1, а биты с 0 по 6 задают количество последующих байтов, которые несут информацию о длине. Например, если первый байт поля указателя длины закодирован как 10000111, то за ним следуют 7 байтов с информацией о длине, а общее количество байтов с информацией о длине равно 8.

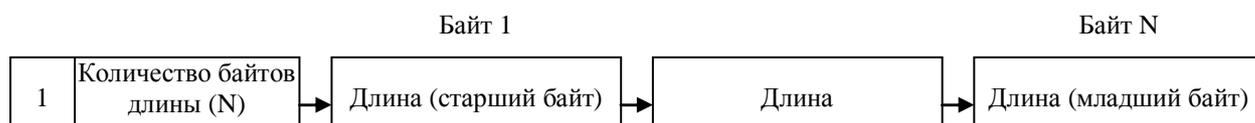


Рис. 2.5. Длинная форма представления поля «длина».

При неопределенной длине поле указателя длины занимает 1 байт (рис. 2.6); все биты с 0 по 6 имеют значение 0, а бит 7 установлен в 1. Однако конец параметра с неопределенной длиной тоже необходимо указать. Для этой цели добавляется специальный маркер конца, конец содержания (ЕОС). Маркер ЕОС состоит из двух байтов, причем все они закодированы нулями. Заметим, что указание неопределенной длины допускается использовать только для параметров типа конструктор. [10]

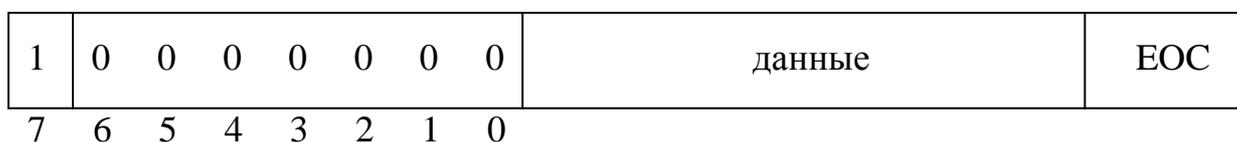


Рис. 2.6. Неопределенная форма представления поля «длина».

Содержание – это сущность элемента ТСАР. Оно содержит информацию, которую элемент передает. Его длина переменна, но всегда содержит целое число байтов. Содержание интерпретируется в зависимости от типа, т.е. в соответствии со значением тега. Поле «содержание» состоит из серии элементов информации порции транзакции, каждый из которых соответствует общему формату «тег, длина, содержание». В случае, когда более чем один элемент информации находится в поле «содержание», то и он использует ту же структуру и сам состоит из тега, длины и содержания. [8]

Если в поле «содержание» присутствует единственное значение, элемент является простым (рис 2.7) [2].



Рис. 2.7. Структура простого информационного элемента ТСАР.

Если же элемент имеет в этом поле другие элементы, он является составным (рис 2.8) [2].

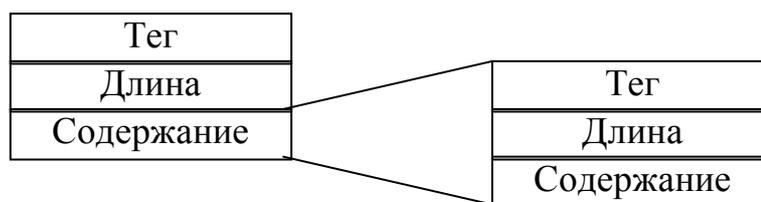


Рис. 2.8. Структура составного информационного элемента ТСАР.

Сообщение ТСАР строится по принципу составного информационного элемента. Оно состоит из транзакционной, диалоговой и компонентной частей. При этом компонентная и диалоговая части сообщения ТСАР являются одними из информационных элементов транзакционной. Организованная таким образом структура сообщения ТСАР представлена на рис. 2.9. [2, 13, 14]

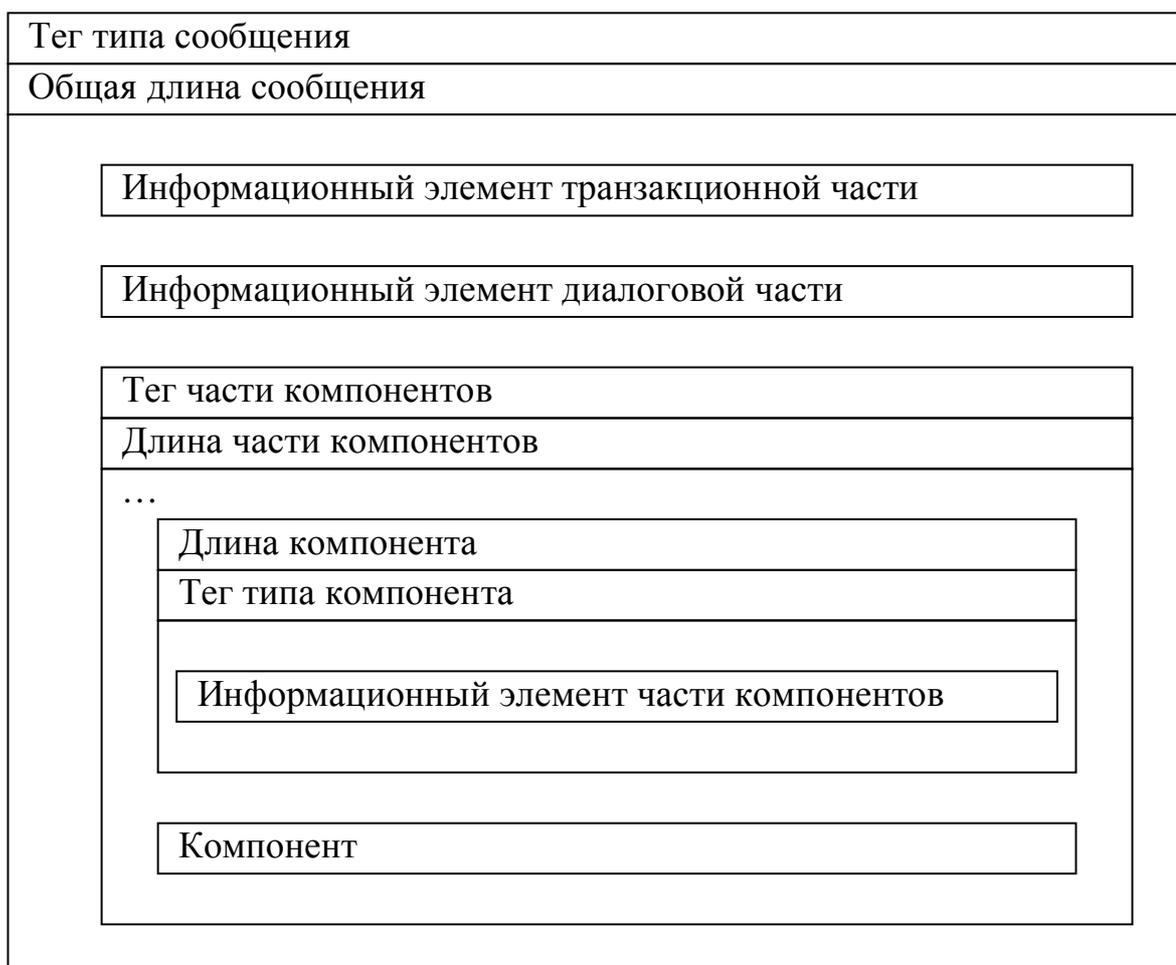


Рис. 2.9. Обобщенная структура сообщения ТСАР

Транзакционная часть включает протокольную управляющую информацию для подуровня транзакции. Информация в части компонентов касается отдельных операций и их ответов. Диалоговая часть является необязательной и

используется для того, чтобы позволить оконечным пунктам соединения синхронизировать обработку данных. [8, 10, 13]

Транзакционная часть сообщения ТСАР может содержать следующие элементы информации [8]:

1. Тип сообщения (существует пять типов сообщений, описание которых было приведено в п.2.2).
2. Общая длина сообщения – указывает число байтов в сообщении.
3. Информационные элементы сообщения – используются только для структурированного диалога. Они включают, например:
  - идентификатор транзакции (ID транзакции) – назначается независимо каждым из двух узлов, взаимодействующих посредством транзакции, позволяя каждому узлу отдельно определять транзакцию и взаимодействовать со всем содержанием сообщения отдельной транзакции. Определяют два типа ID транзакции: ID исходящей транзакции (назначается узлом, посылающим сообщение, и используется для определения транзакции на этом конце) и ID транзакции назначения (идентифицирует транзакцию на принимающем конце). Значение первого принятого ID исходящей транзакции считается ID транзакции назначения;
  - случай C-Сброса - используется, когда подуровень транзакции прерывает транзакцию;
  - информация пользователя о прерывании – используется для передачи информации TR-пользователя, заданной пользователем, когда он прерывает транзакцию.

Диалоговая часть используется для того, чтобы передавать прикладную или пользовательскую информацию. В качестве элемента диалоговой части были определены следующие диалоговые единицы:

- Dialogue Request (запрос диалога). Dialogue Request используется ТС-пользователем в начале транзакции для предложения диалога;
- Dialogue Response (диалоговый ответ). Dialogue Response используется ТС-пользователем в качестве ответа. Эта диалоговая единица посылается в

первом обратном сообщении и содержит информацию о том, принят диалог или нет;

- Dialogue Abort (срыв диалога). Dialogue Abort используется подуровнем компонентов для сообщения ТС-пользователям о непредвиденном прекращении диалога. Также используется ТС-пользователем для завершения диалога в случае аварийно ситуации;
- Dialogue Uni (неструктурированный диалог). Dialogue Uni используется для того, чтобы передавать прикладную или пользовательскую информацию в случае, когда не требуется установления диалога между двумя ТС-пользователями. [10, 13]

Диалоговая часть сообщения ТСАР может содержать следующие элементы информации [10, 13]:

1. Контекстное имя приложения – является ссылкой на определенный набор ТС-пользователей, связанные с ним параметры и любую другую необходимую информацию для взаимодействия двух ТС-пользователей.
2. Версия протокола – указывает версии диалоговой части, которые могут быть поддержаны. При этом каждый бит в поле «версия протокола» представляет какую-либо версию: бит 0 – версию 1, бит 1 – версию 2 и т.д. Если параметр версии протокола отсутствует, то это значит, что подразумевается версия 1.
3. Пользовательская информация – соответствует любой информации, которой обмениваются ТС-пользователи. Ее содержание зависит от значения поля «контекстное имя приложения».
4. Результат – используется подуровнем компонентов для того, чтобы передать ТС-пользователю, инициировавшему диалог, сообщение о результате запроса на установление диалога. Этот параметр может принимать значение «принятый» или «отклоненный».
5. Источник результата диагностики – идентифицирует источник создания параметра «результат». Этот параметр устанавливается подуровнем компонентов и может принимать значение «пользователь диалогового обслуживания» или «поставщик диалогового обслуживания». Если параметр «результат»

имеет значение «принятый», то это значит, что этот параметр устанавливается пользователем диалогового обслуживания. Также параметр «источник результата диагностики» может дополнять «результат» информацией о диагностике.

6. Источник аварийного прекращения работы – определяет инициируется ли непредвиденное прекращение диалога ТС-пользователем или диалоговой частью ТСАР.

Компонентная часть содержит один или более компонентов сообщения. Формат части компонентов содержит длину этой части и отдельные компоненты сообщения. Когда часть компонентов свободна, данный элемент информации не присутствует. Компоненты передаются пользователю на принимающий конец в том же порядке, а котором были получены от пользователя на исходящем конце. [8]

Компонент сообщения состоит из следующих типов элементов информации [8]:

1. Тип компонента (существует пять типов компонентов, описание которых было приведено в п.2.2).
2. Длина компонента – указывает число байтов в компоненте сообщения.
3. Информационные элементы – зависят от типа компонента. Например, ими могут быть:
  - ID вызова – используется как ссылочный номер для однозначного определения запроса на операцию. Он представлен в любом ответе на компонент вызова (возврат результата, возврат ошибки или отклонение), позволяя коррелировать ответ с вызовом;
  - код операции – указывает на конкретную операцию, которая должна быть включена, и присутствует в компоненте INVOKE. Операция может быть местной или общей;
  - набор параметров - используется для составления набора параметров, сопровождающих компонент. Это необходимо в случае, когда более чем один параметр включен в компонент;

- порядок параметров – используется так же, как и элемент «набор параметров», за исключением того, что параметры включаются в компонент в определенной последовательности;
- код ошибки – указывает причину, по которой операция не может быть успешно завершена. Это присутствует только в компоненте RETURN ERROR. Как и в случае операций, ошибки могут быть местными или общими;
- код проблемы – указывает причину отклонения компонента, и один такой компонент присутствует в компоненте отклонения. [8]

Далее сообщение TCAP в закрытом для нижних уровней виде поступает на уровень подсистемы сети, где с использованием соответствующих протоколов SCCP и MTP для него обеспечивается снабжение информацией маршрутизации и осуществляется передача от пункта к пункту до узла назначения. В узле назначения осуществляется обратный процесс раскодировки, распаковки сообщения и анализ информации на уровне ТС-пользователя. [8]

## 2.4. Пользователи TCAP

Подсистема TCAP является прикладным протоколом сети ОКС №7, который используется множеством распределенных приложений. Подсистема TCAP обеспечивает своим пользователям доступ к базам данных и коммутационным станциям через сеть ОКС №7, что позволяет вызывать услуги или модифицировать параметры. [9, 10]

Одной из основных прикладных подсистем ОКС №7, активно внедряемых в последнее время, является прикладная подсистема пользователя интеллектуальной сети INAP [8].

Интеллектуальная сеть – это архитектурная концепция предоставления новых услуг связи, основополагающим требованием к которой является отде-

ление функций предоставления услуг от функций коммутации и распределение их по различным функциональным подсистемам. Функции коммутации остаются в базовой сети связи, а функции управления, создания и внедрения услуг выносятся в создаваемую отдельно от базовой сети «интеллектуальную» надстройку, взаимодействующую с базовой сетью посредством стандартизованных интерфейсов. [6, 8]

Основными компонентами интеллектуальной сети являются узел коммутации услуг (SSP) с интеллектуальной периферией (IP), узел управления услугами (SCP) с базой данных (SDP) и центр администрирования услуг (SMP) с центром программирования услуг (SCEP) [8].

Протокол INAP является протоколом верхнего уровня в системе сигнализации ОКС №7 и обеспечивает взаимодействие между двумя основными объектами телефонной сети, построенной по принципам интеллектуальной сети, а именно между узлом коммутации услуг SSP и узлом управления услугами SCP [6, 8].

Подсистема TCAP обеспечивает возможность реализации широкого диапазона услуг, основанных на обмене информацией между сетевыми компонентами интеллектуальной сети. Для получения услуги интеллектуальной сети пользователь сети набирает номер той АТС, которая обладает функциями узла коммутации услуг, а также код услуги и номер услуги. Подсистема INAP готовит сообщение о запросе услуги и передает его посредством подсистемы TCAP узлу управления услугами и получает необходимую информацию для предоставления услуги и обслуживания вызова. [6, 8, 9]

С помощью использования средств интеллектуальной сети возможно предоставление пользователю в частности таких услуг как:

- «Услуга 800». Эта услуга позволяет вызывающим абонентам осуществлять междугородные телефонные разговоры с оплатой за счет вызываемого абонента. Арендаторами «Услуги 800» являются в основном различные коммерческие фирмы, т.к. данная услуга является эффективным инструментом рекламы и маркетинга. Сам абонентский номер «Услуги 800» в строгом

смысле слова телефонным номером не является. Он представляет собой логический идентификатор всей совокупности оконечных установок, принадлежащих абоненту услуги. Логический номер по определенному алгоритму преобразуется в физический сетевой телефонный номер. Результат этого преобразования может зависеть от целого ряда атрибутов и параметров, назначаемых самим абонентом услуги – местонахождения пользователя, числа и времени суток, поступающей нагрузки и т.д. Эта услуга известна во многих странах мира под различными названиями: «Услуга 130», Green Number, Numero Vert, Linkline, Freephone и т.д. [6, 9]

- Вызов по предоплаченной карте. Данная услуга подразумевает, что при взаиморасчетах с абонентом используется принцип предоплаты с динамическим «списыванием расходов». Внося на счет оператора определенную сумму, абонент получает доступ к услуге по индивидуальному или групповому паролю. Специализированное аппаратное и программное обеспечение, устанавливаемое на узле оператора услуги, автоматически контролирует баланс абонента, не позволяя ему превысить сумму предоплаты. При этом абонент способен получать услугу с любого номера городской телефонной сети. В качестве физического «носителя» услуги операторы чаще всего применяют пластиковые телефонные карточки определенного номинала. [6]
- Вызов по кредитной карте. Эта услуга чаще всего предоставляется корпоративным клиентам и связана с предоставлением услуг телефонной связи в кредит. Алгоритм предоставления услуги аналогичен алгоритму предоставления услуги вызова по предоплаченной карте. База данных проверяет кредитоспособность карты абонента. Расчет с абонентом производится периодически через его счет в банке. [6]
- Телеголосование. Если за предыдущими услугами стоят реальные телефонные номера, по которым, в конечном счете, пользователь услуги, попадает в нужную ему фирму, то услуга «телеголосование» - это всего лишь выход на логику интеллектуальной сети. Таким образом, можно проводить различные опросы населения, викторины и т.д. [6]

Другим пользователем TCAP является протокол поддержки функционирования сотовых телефонных сетей стандарта GSM – прикладная система OKS №7 MAP. Эта подсистема используется для передачи информации роуминга и другой сигнальной информации из одной сотовой сети в другую, а также организует активацию тех или иных операций с удаленного конца. [8]

Оборудование сетей стандарта GSM содержит следующие элементы [8]:

- коммутационный центр подвижной связи (MSC) – выполняет функции установления соединения как между подвижными абонентами сети, так и между абонентами СПС и ТфОП;
- базовая станция (BS) – реализует радиointерфейс с подвижными абонентом;
- контроллер базовых станций (BSC) – обеспечивает управление базовыми станциями и связь с коммутационным центром;
- домашний регистр местоположения (HLR) – содержит базу данных об абонентах, зарегистрированных в данном коммутационном центре;
- гостевой регистр местоположения (VLR) – содержит базу данных об абонентах, посетивших зону обслуживания данного коммутационного центра;
- центр аутентификации (AC) – обеспечивает проверку полномочия подвижного абонента и осуществления его доступа к сети связи;
- регистр идентификации оборудования (EIR) – содержит базу данных, необходимых для управления идентификацией оборудования.

Подсистема MAP реализована в MSC, HLR, VLR и EIR. Она обеспечивает их взаимодействие между собой. Также подсистема MAP используется для передачи информации роуминга и другой сигнальной информации из одной сотовой сети в другую. [5]

Подсистема MAP обеспечивает не только передачу информации между сотовыми системами, но и организует активацию тех или иных операций с удаленного конца. Например, при поступлении определенных сообщений из другой сотовой сети активизируются услуги сотовой сети, которой принадлежит вызывающий абонент, а также сообщаются в обратном направлении результаты активации тех или иных услуг. [5]

К основным процедурам MAP относятся [5, 8]:

- регистрация местоположения абонента для сохранения возможности осуществления исходящих и приема входящих вызовов в пределах всей сети, что обеспечивает возможность роуминга;
- регистрация и стирание предыдущей информации о местоположении абонента;
- дополнительные виды обслуживания;
- сохранение абонентских данных в регистрах HLR и VLR;
- выдача информации о тарификации и др.

Еще одним приложением, использующим средства транзакции, является подсистема эксплуатации, технического обслуживания и администрирования OMAP, которая определяет функции, процедуры и логические объекты для эксплуатации, техобслуживания и управления сетью ОКС №7 и взаимодействует со всеми уровнями системы сигнализации. Функции управления и техобслуживания сети ОКС №7 могут использовать систему сигнализации в качестве механизма переноса данных. [8]

Подсистема OMAP позволяет персоналу техобслуживания и эксплуатации контролировать и управлять оборудованием, связанным с сетью сигнализации ОКС №7, из центра технической эксплуатации с помощью протокола, обеспечивающего средства обмена со всеми другими узлами сети. Для обеспечения передачи информации, не относящейся к информационному каналу, между пунктом управления и узлом (узлами), задействованными для обеспечения функций технического обслуживания и эксплуатации сети, используется подсистема TCAP. [8]

Выводы по главе. Подсистема TCAP относится к верхнему уровню системы ОКС №7 и обеспечивает (совместно с SCCP и MTP) передачу через сеть информации, не относящейся к каналу. Функции подсистемы TCAP образуют два подуровня: подуровень компонентов и подуровень транзакции. Подуровень компонентов обеспечивает возможность обмена компонентами между ТС-

пользователями. Существуют компоненты пяти типов: INVOKE, RETURN RESULT NOT LAST, RETURN RESULT LAST, RETURN ERROR, REJECT. Последовательность компонентов, которыми обмениваются ТС-пользователи, образует диалог. Диалог может быть структурированным и неструктурированным. Подуровень транзакций обеспечивает возможность обмена сообщениями, содержащими компоненты, между ТС-пользователями, используя услуги нижележащих уровней. Сообщения TCAP бывают следующих типов: UNIDIRECTIONAL, BEGIN, CONTINUE, END, ABORT. Сообщение TCAP состоит из информационных элементов, расположенных в нем по определенному правилу, и делится на три части: транзакционную, диалоговую и компонентную. При этом компонентная и диалоговая части сообщения TCAP являются одними из информационных элементов транзакционной. Подуровень транзакции также поддерживает режимы структурированного и неструктурированного диалога. Подсистема TCAP используется многими приложениями для реализации широкого спектра услуг, таких как услуга «800», телеголосование, роуминг и др.

## Глава 3. Тестирование протокола ТСАР

### 3.1. Тестовая спецификация протокола ТСАР

Принципы тестирования подсистемы ТСАР определены в рекомендации МСЭ Q.787. Эта рекомендация содержит полный набор тестов для подсистемы ТСАР системы сигнализации ОКС №7. Выполняя эти тесты при испытании реальных систем телекоммуникации, пользователь может проверить функциональные возможности подсистемы ТСАР, анализируя сообщения ТСАР и их содержание. [15]

Рекомендация Q.787 разделена на две части: спецификация по тестированию подуровня транзакции и спецификация по тестированию подуровня компонентов. При этом тестировать эти подуровни следует вместе, т.к. большинство их функций связаны между собой. [15]

Для проверки реализации протокола ТСАР в тестовое окружение должны входить подсистемы МТР и SССР, предварительно прошедшие тестирование, а также:

- тестер ТСАР, который требуется для симуляции операций протокола ТСАР и генерации сообщений ТСАР;
- стабильная сигнальная связь между всеми точками ТСАР;
- монитор сообщений ТСАР, который требуется для просмотра и сохранения последовательности сообщений ТСАР и их параметров при работе тестируемой среды в нормальных и в нештатных ситуациях.

Для проверки корректности реализации протокола ТСАР требованиям соответствующих стандартов на систему сигнализации ОКС №7 существуют спецификации двух типов тестов: проверки соответствия (VAT) и проверки совместимости (СРТ) [4].

Тесты соответствия (VAT) предназначены для проверки реализации одного протокола в тестируемой системе на соответствие спецификациям международных или национальных стандартов [4].

Тесты совместимости (CPT) предназначены для проверки правильности взаимодействия двух или более реализаций одного протокола, выполненных в соответствии со спецификациями международных или национальных стандартов [4].

Тесты VAT всегда предшествуют проверке совместимости CPT и выполняются в пункте сигнализации, не находящемся в обслуживании. Для выполнения тестов VAT необходимо использовать симулятор встречного пункта сигнализации. В тестовых спецификациях тестируемый пункт сигнализации обозначается как SP A. [4]

Целью тестов CPT является проверка корректности взаимодействия между реализациями протокола в пунктах сигнализации разных производителей или при замене версии программного обеспечения в одном из взаимодействующих пунктов одного производителя. Тестирование совместимости может проводиться не только во вновь вводимом пункте сигнализации, но также и в пункте, уже введенном в обслуживание. При проведении тестов CPT все входящие в тестовую конфигурацию пункты сигнализации представляют собой одну тестируемую систему. [4]

Тестовые конфигурации для тестов типов VAT и CPT схожи, но не идентичны. При проведении тестов VAT тестируемый пункт включается в тестовую среду и становится частью тестовой конфигурации. Тестовая конфигурация при этом должна удовлетворять следующим трем критериям:

- тестируемый пункт подсоединяется к тестовой среде одним или несколькими пучками звеньев;
- имеется возможность генерации и приема тестовой нагрузки;
- имеются возможности выполнения теста и средства хранения и подробного анализа сообщений. [4]

При проведении тестов СРТ все пункты сигнализации объединяются в одну большую тестируемую систему, которая должна удовлетворять следующим четырем требованиям:

- пункты тестируемой системы соединяются друг с другом одним или несколькими пучками звеньев;
- имеется возможность генерации и приема тестовой и реальной нагрузки;
- имеются возможности выполнения тестов, заданных спецификациями по тестированию, и средства хранения и подробного анализа сообщений;
- имеются возможности мониторинга процесса обслуживания вызова и наблюдения за каналами. [4]

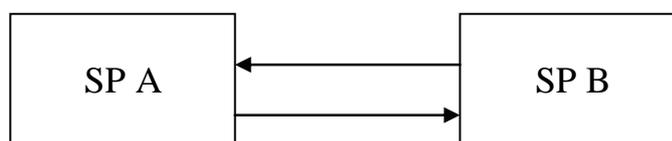


Рис. 3.1. Конфигурация 1.

Для проведения тестов протокола ТСАР требуется только один вид тестовой конфигурации, который показан на рис. 3.1. [15]

НОМЕР ТЕСТА: 1.1.1.1	
ССЫЛКА: Q.774 раздел 3.3.3.1.1	
ЗАГОЛОВОК: Нормальное функционирование; неструктурированный диалог	
ПОДЗАГОЛОВОК: Посылает сообщение тестируемая сторона.	
ЦЕЛЬ: Проверить, что пункт сигнализации А может корректно посылать однонаправленные сообщения.	
УСЛОВИЯ ПРОВЕДЕНИЯ ТЕСТА: SP A (TSL) и SP B (TSL) в незанятом состоянии	
КОНФИГУРАЦИЯ: 1	ТИП ТЕСТА: VAT и СРТ
ОЖИДАЕМАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ СИГНАЛЬНЫХ СООБЩЕНИЙ:	
SP A (TSL)	
<i>TR-UNI req.</i>	
=====>	
<b>UNIDIRECTIONAL</b> —————>	
ОПИСАНИЕ ТЕСТА	
1.	Послать однонаправленное сообщение из SP A в SP B.
2.	ПРОВЕРКА А: Убедится, что однонаправленное сообщение было послано из SP A корректно.
3.	ПРОВЕРКА В: Убедится, что все приборы SP A, связанные с осуществлением транзакции, после завершения транзакции были приведены в исходное состояние.
ПРОВЕРОЧНАЯ ТАБЛИЦА ДЛЯ ИНФОРМАЦИОННЫХ ЭЛЕМЕНТОВ СООБЩЕНИЯ	
ОДНОНАПРАВЛЕННОЕ	
Message type tag: 01100001	
Message type length: correct number of octets	
Component portion tag: 01101100	
Component portion length: correct number of octets	

Рис. 3.2. Описание теста подсистемы ТСАР для неструктурированного диалога при нормальном функционировании системы.

На рис. 3.2. представлен пример описания одного из тестов в рекомендации Q.787. Для каждого теста приводится подробное описание, включая его заголовок, цель, предварительные условия, конфигурацию, типы пунктов сигнализации, тип теста, ссылки на соответствующие параграфы рекомендации по протоколу TCAP, ожидаемую последовательность сообщений, описание проведения теста, проверочную таблицу для информационных элементов сообщения. При этом в некоторых тестах на диаграмме ожидаемой последовательности сообщений, кроме непосредственно самих сообщений, показаны соответствующие примитивы, что сделано только для простоты понимания. [4, 15]

## 3.2. Язык MSC

Существует несколько способов описания телекоммуникационных архитектур. Одним из таких способов является описание на языке MSC. Как правило, описания процессов на языке MSC сопровождают описания на языке SDL в виде карт последовательностей сообщений. Язык MSC также дает возможность предварительного описания процессов на фазе подготовки SDL-спецификаций. Представления в форме MSC обладают большой наглядностью и могут переводиться в SDL форму. При этом возникает также и обратная задача перевода из SDL в MSC, что особо важно при отладке готового программного обеспечения и тестировании протоколов. [2]

Основное использование MSC – создание сценариев обмена сигналами между различными процессами или объектами. Именно по набору такого рода сценариев проводится проверка правильности отработки протоколов сигнализации и в частности протокола TCAP. MSC-описания легко использовать в качестве шаблонов, по которым работают имитаторы программного обеспечения обработки вызовов и протокол-тестеры систем сигнализации. [2]

MSC-сценарии могут быть представлены в текстовом и графическом виде. Текстовое описание, как правило, представляет собой информационное объяснение на мета-языке, строящемся на формах Бэкуса-Наура. [2, 16]

Для графического описания протоколов сигнализации применяются следующие элементы языка MSC [2]:

1. Момент (Instance).
2. Сообщение (Message).
3. Вентиль (Gate).
4. Таймер (Timer).

В пределах MSC-сценария определены моменты. Начальный символ момента определяет начало описания случая в пределах MSC-сценария, но не описывает создание этого момента. Соответственно, конечный символ момента определяет конец описания случая в пределах этого MSC-сценария, но не описывает завершение данного случая. [16]

Сообщение в пределах MSC-сценария показывает связь между компонентами системы, также компонентами системы и окружающей средой. Посылка и прием сообщений – это два асинхронных события. Это предполагает, что в MSC окружающая среда способна принимать и посылать сообщения независимо. В графическом описании сообщение представлено стрелкой. Потеря сообщения, то есть случай, когда сообщение посылается, но не принимается, может быть обозначена ключевым словом, потерянном в текстовом представлении и пустым отверстием около окончания стрелки в графическом представлении. Аналогично, спонтанно найденное сообщение, то есть сообщение, которое появляется ниоткуда, может быть определено ключевым словом, найденным в текстовом представлении и пустым отверстием около начала стрелки в графическом представлении. [2, 16]

Вентиль представляет собой интерфейс между MSC и его окружающей средой. Любое сообщение, приложенное к структуре MSC, попадает внутрь через вентиль. Вентили всегда имеют название. [16]

В MSC может использоваться установка таймера с последующим прерыванием из-за истечения времени или установка таймера с последующего сбросом. В графическом представлении символ таймера представляет собой песочные часы. [16]

Основные символы, используемые в MSC, приведены в приложении 3.

Недостаток описания с помощью MSC заключается в его линейном характере и в невозможности представить на одной диаграмме ветвление алгоритма [2].

К достоинствам описания процессов при помощи MSC относятся наглядность и легкость, с которой могут быть проверены протоколы, специфицированные таким методом. Достаточно сказать, что тестовые сценарии получаются путем слияния MSC-спецификаций разрабатываемого процесса и имитатора протокола. [2]

Именно таким образом разработаны протокол тестеры российских систем сигнализации, используемые для отладки программного обеспечения цифровых АТС. С помощью этих протокол-тестеров сообщения о сбое в сценарии, поступающие оператору, позволяют провести не только проверку, но и отладку указанного программного обеспечения. [2]

### **3.3. Тестовая платформа SNT**

Отладка и тестирование программно-аппаратных средств реализации протоколов сигнализации являются одними из наиболее трудоемких и ответственных задач при разработке новых и адаптации существующих коммутационных узлов и станций. В связи с этим чрезвычайно важно наличие эффективных программно-аппаратных средств тестирования протокольных реализаций систем сигнализации. [2]

Платформа тестирования SNT является универсальным инструментом для проведения всех видов тестирования коммутационного оборудования и интегральной оценки параметров качества работы сотовых и фиксированных сетей связи, а также сетей NGN. Этот тестер выполняет синтез параметров передаваемых сигналов, измерение параметров принимаемых сигналов, анализ результатов измерений и вывод результатов. Элементы платформы, в том числе, обеспечивают поддержку протоколов ОКС №7. [2, 11]

Тестирование протоколов сигнализации включает в себя тестирование соответствия, диагностическое тестирование и оценку производительности. Каждый этап тестирования представлен соответствующим программным или программно-аппаратным модулем. Протокол-тестер SNT реализует все необходимые логические функции анализа конкретных протоколов сигнализации в трех основных режимах: ручном, параметрическом и статистическом. [2, 11]

В режиме ручного тестирования оператор сам выбирает конкретные сценарии и управляет последовательностью действий. В режиме автоматического и/или параметрического тестирования оператор заранее настраивает те или иные сценарии, потом запускает протокол и распечатывает результаты.[2]

Аппаратная часть протокол-тестера SNT представляет собой процессорную систему, базирующуюся на портативном компьютере и содержащую следующие функциональные подсистемы: управляющую подсистему, подсистему визуализации данных, аппаратные интерфейсы протоколов сигнализации, диалоговую подсистему и др. [2]

Подсистема визуализации обеспечивает представление тестовой диагностической информации на экране монитора, в том числе и в виде отметок в заранее выбранных сценариях MSC [2].

Управляющая подсистема выполняет все основные логические функции симуляции и анализа обмена сигналами в соответствии с протоколом сигнализации. Эта же подсистема управляет работой других связанных с ней подсистем и обеспечивает мониторинг, диспетчеризацию приема/передачи сигналов, а также контроль состояния интерфейса (определение моментов появления тех

или иных сигналов). Она же включает в себя наборы тестов, предназначенных для проверки логики сигнализации, контролирует время обработки сигналов, анализирует допустимость последовательностей сигналов, а также обеспечивает возможность передачи заведомо ошибочных команд в соответствии с выбранным сценарием тестирования протокола. [2]

Для тестирования сетевых элементов, использующих для взаимодействия между собой протокол TCAP, применяется протокол-тестер SNT-7531. (рис. 3.3). SNT-7531 – протокол-тестер современных телекоммуникационных протоколов, включая подсистемы и прикладные протоколы общеканальной системы сигнализации №7 (MTP, SCCP, ISUP, TCAP, MAP, MUP, HUP). Протокол-тестер SNT-7531 обеспечивает детальный анализ протоколов в соответствии с национальными и международными рекомендациями и стандартами. Программное обеспечение SNT-7531 позволяет контролировать процесс тестирования, осуществлять необходимые настройки, получать контекстную помощь как по специфике тестируемых протоколов, так и по самой системе тестирования, сохранять и распечатывать результаты тестов. [11]



Рис. 3.3. Протокол-тестер SNT-7531.

Протокол-тестер SNT-7531 может работать в режиме мониторинга и симуляции, что позволяет использовать его приборы на всех этапах жизненного цикла телекоммуникационного оборудования [11].

В режиме мониторинга пользователю предоставляется возможность отслеживать необходимую информацию в ходе тестирования, используя фильтрацию по типу сообщения, исходящему пункту сигнализации, входящему пункту сигнализации и т.д. Полученный трейс можно сохранить в двоичном виде или текстовом виде с возможностью дальнейшего просмотра в других приложениях (Microsoft Word, Norton, FAR и т.д.) и вывода на печать. Для получения общего представления о состоянии звена сигнализации пользователю предоставляется возможность сбора статистики на базе полученных трейсов. Пользовательский интерфейс содержит два основных конфигурируемых экранных элемента: основное окно мониторинга и вспомогательное окно мониторинга. Основное окно мониторинга используется для вывода декодированных сообщений в полном виде. Вспомогательное окно мониторинга предназначено для отслеживания последовательности приходящих сообщений и быстрого просмотра основных полей. [11]

В режиме симуляции прибор SNT-7531 имеет возможность имитации работы станции по заранее заданным тестовым сценариям. Комплект стандартных тестовых сценариев выполнен в соответствии с рекомендацией МСЭ. Если сценарий и параметры установок не содержат логических ошибок, то после загрузки в окне симулятора отобразится ход обмена сообщениями выбранного сценария. Кроме сообщений появляются комментарии, поясняющие цель данного теста. Сразу после загрузки становятся доступны команды запуска сценария и команда пошагового выполнения в управляющем меню и на панели инструментов. В процессе исполнения сценария последовательно выполняются все действия, описанные в сценарии. Процедуру исполнения сценария в любой момент можно прервать командой остановка или приостановить командой пауза. В режиме паузы возможно пошаговое выполнение сценария для более детального анализа тестируемого оборудования. Все сообщения, поступающие в симулятор в режиме паузы, помещаются во временную очередь и хранятся там до очередного запуска. В любой момент имеется возможность узнать о результатах выполненных сценариев. [11]

Целесообразность применения протокол-тестеров в каждом конкретном случае определяется практикой. Но, по крайней мере, две области применения обеспечивают высокую эффективность использования протокол-тестеров: отладка программно-аппаратных средств реализации протоколов сигнализации в коммутационных узлах и решение конфликтных ситуаций при установке новых систем коммутации в окружении существующих аналоговых и цифровых АТС предыдущих поколений. [2]

Выводы по главе. Тестирование подсистемы ТСАР проводится в соответствии с рекомендацией МСЭ Q.787, которая содержит полный набор тестов для подсистемы ТСАР системы сигнализации ОКС №7. Выполняя эти тесты при испытании реальных систем телекоммуникации, пользователь может проверить функциональные возможности подсистемы ТСАР, анализируя сообщения ТСАР и их содержание. Для тестирования сетевых элементов, использующих для взаимодействия между собой протокол ТСАР, применяется протокол-тестер SNT-7531. Существуют два способа тестирования сетевых элементов: в режиме мониторинга и режиме симуляции. В режиме мониторинга осуществляется наблюдение за работой узлов связи. В режиме симуляции прибор SNT-7531 имеет возможность имитации работы станции по заранее заданным тестовым сценариям. Для написания сценариев обмена сигналами между различными узлами связи используют язык MSC. MSC-описания легко использовать в качестве шаблонов, по которым работают имитаторы программного обеспечения обработки вызовов и протокол-тестеры систем сигнализации.

## Глава 4. Разработка тестовых сценариев ТСАР

### 4.1. Тестовые сценарии для услуги «800»

Услуга «800» предоставляет пользователю телефонной сети возможность бесплатной связи с одним из нескольких терминалов абонента этой услуги путем набора единого логического номера. Терминалы абонента услуги могут размещаться в разных пунктах территории, обслуживаемой телефонной сетью, быть включенными в разные АТС этой сети и иметь разные физические номера, а правила пересчета логического номера в тот или иной физический номер определяются критериям, который назначает абонент услуги. Вызов по номеру «800» из той или иной точки ТфОП может маршрутизироваться в зависимости от времени суток, дня недели, номера вызывающего абонента, специфических требований абонента – владельца номера, поступающей нагрузки и т.п. В случае занятости или при отсутствии ответа маршрутизация может отличаться от маршрутизации при наличии ответа. Кроме того, логика услуги может предусматривать подачу вызывающему пользователю речевых сообщений и акустических сигналов. [3]

При обращении к услуге «800» пользователь набирает код доступа к интеллектуальной сети, код доступа к услуге и, далее, логический номер абонента услуги. В телефонных сетях России обращение к услуге «800» осуществляется набором номера вида: Пр – 800 –  $X_1 X_2 \dots X_n$ , где:

Пр – префикс, равный:

8 – если выход к платформе интеллектуальной сети осуществляется через АМТС;

0 – если выход к платформе интеллектуальной сети осуществляется через УСС;

800 – код доступа к услуге «800»;

$X_1 X_2 \dots X_n$  – логический номер абонента услуги «800». [3]

Для тестирования сетевых элементов, использующих для взаимодействия между собой протокол ТСАР (в данном случае SSP и SCP), применяется

протокол-тестер SNT-7531. В режиме симуляции протокол-тестера SNT-7531 возможна имитация одного из сетевых элементов для проверки работы другого по заранее заданным тестовым сценариям.

Пусть протокол-тестера SNT-7531 в режиме симуляции выполняет функции узла управления услугами SCP. Тогда по следующим тестовым сценариям возможна проверка функционирования подсистемы TCAP узла SSP при предоставлении услуги «800».

Сделаем допущение, что при рассмотрении следующих алгоритмов выход к платформе интеллектуальной сети осуществляется через АМТС, а на участке между АТС, с которой поступает вызов, и АМТС используется система сигнализации ОКС №7.

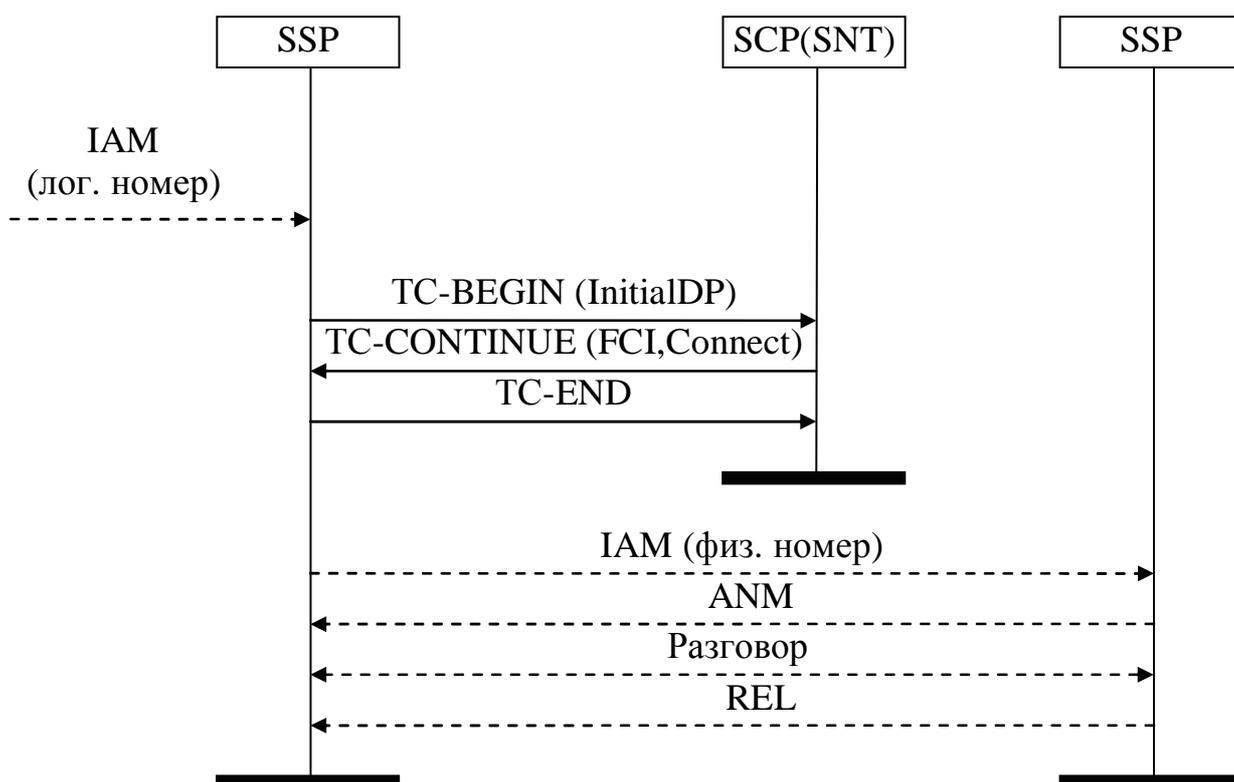


Рис. 4.1. Сценарий тестирования подсистемы TCAP узла SSP при предоставлении услуги «800»

Сценарий тестирования подсистемы TCAP узла SSP при предоставлении услуги «800» (рис. 4.1) содержит следующие шаги:

1. На основании набранных пользователем цифр 8 – 800 –  $X_1 X_2 \dots X_n$  оконечная АТС направляет сообщение IAM, которое содержит логический номер вызываемого абонента, к АМТС с функциями SSP.
2. Обнаружив, что вызов связан с обращением к услуге интеллектуальной сети, SSP приостанавливает процесс его обслуживания и инициирует сеанс связи с узлом SCP, т.е. готовит соответствующий запрос в виде сообщения INAP InitialDP. В случае вызова услуги «800» операция InitialDP обязательно содержит параметр Service Key со сведениями о типе услуги, информацию о набранных пользователем цифрах номера, а также о номере самого пользователя.
3. Подсистема INAP в свою очередь передает этот запрос подсистеме TCAP. Подсистема TCAP принимает и обрабатывает этот запрос, при этом формируется сообщение TC-BEGIN. Передачей этого сообщения TCAP открывает диалог одной подсистемы INAP с другой.
4. Затем сообщение TC-BEGIN направляется к подсистеме SCCP, посредством которой оно передается по сети. Подсистема SCCP маршрутизирует сообщения TCAP через пункты STP на основании адресной информации.
5. Подсистема TCAP запрашиваемого узла SCP принимает и обрабатывает сообщение TC-BEGIN. Затем TCAP отправляет запрос на выполнение операции InitialDP подсистеме INAP. Подсистема INAP анализирует параметр Service Key, в результате чего операция направляется к приложению, обслуживающему услугу «800».
6. Используя логический номер абонента услуги «800», SCP определяет номер его счета и информирует SSP об организации начисления оплаты и о физическом вызываемом номере ТфОП с помощью операций INAP FurnishChargingInformation и Connect, которые передаются в сообщении TC-CONTINUE.
7. Далее SSP заканчивает транзакцию посредством посылки сообщения TC-END.
8. Приостановленный процесс обслуживания вызова в SSP возобновляется. В соответствии с данными, полученными от SCP, SSP посылает сообщение

IAM, в котором указывается физический номер вызываемого абонента, входящей АМТС.

Теперь рассмотрим сценарий тестирования (рис. 4.2.), когда подсистема TCAP прерывает транзакцию:

1. На основании набранных пользователем цифр  $8 - 800 - X_1 X_2 \dots X_n$  оконечная АТС направляет сообщение IAM, которое содержит логический номер вызываемого абонента, к АМТС с функциями SSP.
2. Обнаружив, что вызов связан с обращением к услуге интеллектуальной сети, SSP приостанавливает процесс его обслуживания и инициирует сеанс связи с узлом SCP, т.е. готовит соответствующий запрос в виде сообщения INAP InitialDP.
3. Подсистема INAP в свою очередь передает этот запрос подсистеме TCAP. Подсистема TCAP принимает и обрабатывает этот запрос, при этом формируется сообщение TC-BEGIN. Затем это сообщение направляется к подсистеме SSCP, которая маршрутизирует данное сообщение через пункты STP.
4. Подсистема TCAP запрашиваемого узла SCP принимает и обрабатывает сообщение TC-BEGIN. В случае если подсистема TCAP обнаружила какую-либо ошибку в сообщении, она передает информацию об этом SSP в сообщении TC-P-ABORT. При этом в сообщении могут указываться следующие причины прерывания процесса:
  - неизвестный тип сообщения;
  - неизвестный тип компонента;
  - несуществующий идентификатор исходящей транзакции;
  - принятое сообщение неправильно закодировано;
  - принятое сообщение неправильно структурировано;
  - недостаток средств для начала транзакции.
5. Процесс обслуживания вызова в SSP прерывается, а к АТС посылается сообщение REL.

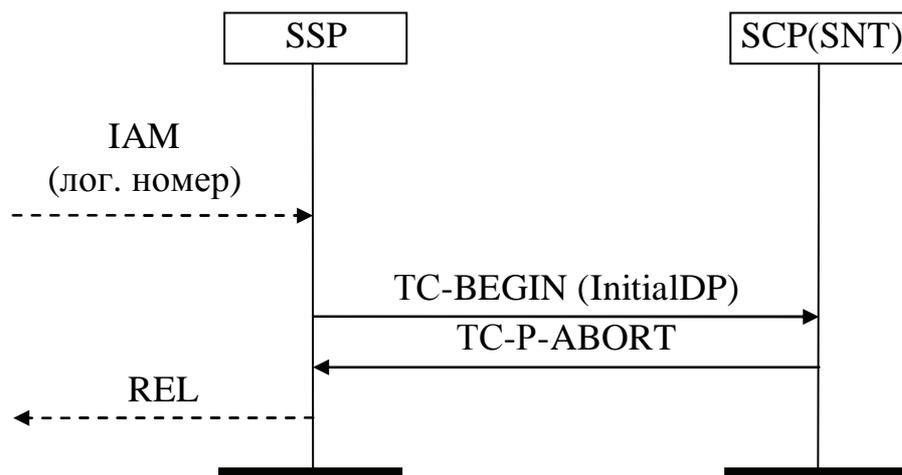


Рис. 4.2. Сценарий предоставления услуги «800», при котором подсистема TCAP прерывает транзакцию.

## 4.2. Тестовые сценарии для услуги «телеголосование»

Услуга «телеголосование» позволяет проводить опрос общественного мнения с использованием ресурсов телефонной сети. В соответствии с числом вариантов предлагаемых ответов назначаются логические номера, а участники голосования набирают тот номер, который соответствует их мнению. Один из каждых  $N$  вызовов может быть направлен в студию, откуда ведется трансляция теле- (или радио-) программы, для проведения диалога голосующего пользователя с ведущим. Средствами интеллектуальной сети производится подсчет числа вызовов, поступивших на каждый номер, и предоставление администратору и абоненту услуги доступа к результатам опроса. Голосование может быть премиальным. В этом случае один или несколько абонентов, первыми правильно ответивших на вопрос, получают приз или денежное вознаграждение. [3]

Услуга «телеголосование» предоставляется абоненту на определенный период времени по договоренности с поставщиком услуги. Для проведения го-

лосования администратор услуги определяет необходимые параметры в соответствии с ее профилем. Среди основных параметров услуги, определяемых администратором, можно выделить число логических номеров, доля вызовов, подлежащих просеиванию, периодичность передачи данных в SCP и временной интервал между сообщениями, посылаемыми из SCP в SMP. [3]

В телефонных сетях России вызов услуги «телеголосование» осуществляется набором номера  $Pr - 803 - X_1 X_2 \dots X_n$ , где

$Pr$  – префикс, равный:

8 – если выход к платформе интеллектуальной сети осуществляется через АМТС;

0 – если выход к платформе интеллектуальной сети осуществляется через УСС;

803 – код доступа к услуге «телеголосование»;

$X_1 X_2 \dots X_n$  – логический номер абонента услуги «телеголосование». [3]

Для тестирования сетевых элементов, использующих для взаимодействия между собой протокол TCAP (в данном случае SSP и SCP), применяется протокол-тестер SNT-7531. В режиме симуляции протокол-тестера SNT-7531 возможна имитация одного из сетевых элементов для проверки работы другого по заранее заданным тестовым сценариям.

Пусть протокол-тестера SNT-7531 в режиме симуляции выполняет функции узла управления услугами SCP. Тогда по следующим тестовым сценариям возможна проверка функционирования подсистемы TCAP узла SSP при предоставлении услуги «телеголосование».

Сделаем допущение, что при рассмотрении следующих алгоритмов выход к платформе интеллектуальной сети осуществляется через АМТС, а на участке между АТС, с которой поступает вызов, и АМТС используется система сигнализации ОКС №7.

Рассмотрим (рис. 4.3) тестовый сценарий подсистемы TCAP узла SSP при предоставлении услуги «телеголосование»:

1. Перед началом процедуры подсистема INAP соответствующего SCP формирует и передает подсистеме TCAP запрос на выполнение операции

ActivateServiceFiltering, которая определяет время начала и окончания опроса, критерий просеивания и тип обслуживания, применяемого к отсеянным и просеянным вызовам. Во время действия операции фильтрации соединения, соответствующие вызовам на определенные для голосования номера, устанавливаются только до SSP, где производится подсчет вызовов на каждый из номеров.

2. Подсистема TCAP создает сообщение TC-BEGIN, в котором передает данный запрос. SCP передает это сообщение по сети посредством подсистемы SCCP ко всем SSP. Этим сообщением открываются диалоги между подсистемой INAP SCP и подсистемами INAP всех SSP, при этом каждому диалогу присваивается свой идентификатор.
3. Подсистема TCAP SSP принимает и обрабатывает это сообщение, а затем передает запрос на операцию ActivateServiceFiltering подсистеме INAP.

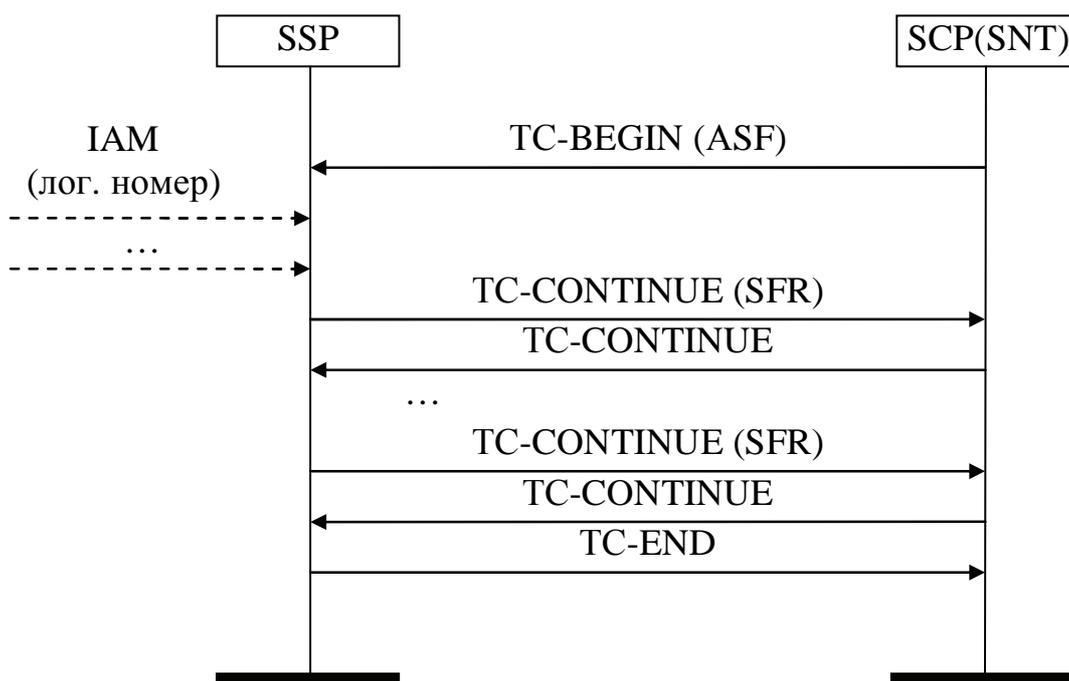


Рис. 4.3. Тестовый сценарий подсистемы TCAP узла SSP при предоставлении услуги «телеголосование».

4. После начала опроса на АМТС с функциями SSP начинают поступать сообщения IAM от входящих АТС, в которых указывается логический номер вы-

зываемого абонента. Подсистема INAP распознает номер услуги «телеголосование» и накапливает результаты.

5. Через заданные промежутки времени SSP посылают текущие результаты опроса в SCP при помощи операций INAP ServiceFilteringResponse. Для этого формируется сообщение TCAP TC-CONTINUE, в котором передается данная операция. SCP собирает и накапливает данные от SSP и посылает их к SMP, куда заказавший опрос абонент может обратиться за получением отчета о результатах голосования.
6. По окончании опроса SSP посылает SCP сообщение TC-END.

Далее рассмотрим сценарий, при котором пользователь TCAP (в данном случае подсистема INAP) прерывает транзакцию (рис. 4.4):

1. Перед началом голосования подсистема INAP соответствующего SCP формирует и передает подсистеме TCAP запрос на выполнение операции ActivateServiceFiltering, которая определяет время начала и окончания опроса, критерий просеивания и тип обслуживания, применяемого к отсеянным и просеянным вызовам.
2. Подсистема TCAP создает сообщение TC-BEGIN, в котором передает данный запрос. SCP передает это сообщение по сети посредством подсистемы SCCP ко всем SSP.
3. Подсистема TCAP SSP принимает и обрабатывает это сообщение, а затем передает запрос на операцию ActivateServiceFiltering подсистеме INAP.
4. Предположим, что подсистема INAP SCP решила по каким-либо причинам прервать транзакцию. Тогда подсистема TCAP формирует сообщение TC-U-ABORT и посредством SCCP рассылает его всем SCP. При этом причина прерывания может сообщаться, а может не сообщаться. В случае, если пользователю требуется передать причину прерывания, то эта информация содержится в диалоговой части сообщения.

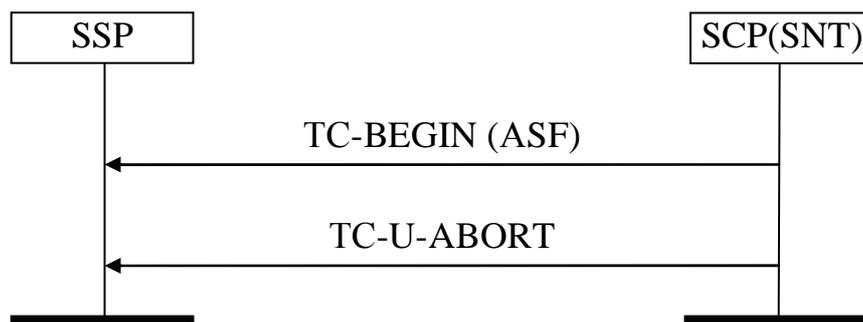


Рис. 4.4. Сценарий предоставления услуги «телеголосование», при котором пользователь ТСАР прерывает транзакцию.

### 4.3. Тестовые сценарии для услуги «роуминг»

Для пользователей сетей подвижной связи (СПС) подсистема ТСАР, среди прочего, поддерживает организацию роуминга. Этот термин происходит от английского глагола to roam (бродить) и подразумевает предоставление абонентам сотовой сети возможности пользоваться связью за пределами зоны действия оператора, обслуживающего этих абонентов. Протоколом поддержки роуминга мобильных абонентов сотовой телефонной сети является прикладная подсистема MAP.

Для реализации роуминга мобильному абоненту сети стандарта GSM присваиваются следующие основные номера и идентификаторы:

1. Международный идентификатор мобильного абонента (IMSI), который записывается в постоянное запоминающее устройство SIM-карты.
2. Номер сети общего пользования, который соответствует телефонной нумерации каждой сети оператора мобильной связи.
3. Временный роуминговый номер (MSRN), который выделяется при установлении входящего соединения к абоненту-роумеру на время установления со-

единения, но не более 30 секунд. Блок номеров MSRN выделяется из общей телефонной нумерации сети. [5, 7]

Для организации такой услуги, помимо необходимости существования в регионах сотовых систем, действующих в том же стандарте GSM и имеющих межоператорские коммерческие соглашения с исходной операторской компанией, требуется постоянно обновлять сетевую базу данных для того, чтобы хранить в ней сведения о текущем местоположении абонентов. В составе сети GSM существуют два вида баз данных: HLR и VLR.

Регистр HLR является справочной базой данных о постоянно зарегистрированных в сети абонентах. В ней содержатся опознавательные адреса и номера, а также параметры подлинности абонентов, состав услуг связи, информация о маршрутизации, данные о роуминге абонента (включая данные о временном идентификационном номере абонента и соответствующем VLR). Каждому абоненту может присваиваться несколько идентификаторов, включая международный идентификатор мобильного оборудования IMEI, международный идентификатор мобильного абонента IMSI, временный идентификатор мобильного абонента TMSI и ISDN-номер мобильной станции MSISDN. В HLR хранится та часть информации о местоположении какого-либо мобильного абонента, которая позволяет MSC доставить вызов. Информация о местоположении абонента должна обновляться в регистре HLR каждые несколько минут. По мере перемещения абонента из одной зоны в другую содержимое HLR постоянно обновляется с помощью сообщений TCAP. Такой механизм позволяет мобильному абоненту абсолютно свободное передвижение в пределах всей сети без риска потерять входящие вызовы. [5, 8]

Регистр VLR представляет собой локальную базу данных об абоненте для той зоны, где он находится, что позволяет исключить постоянные запросы в HLR. С его помощью достигается функционирование подвижной станции за пределами контролируемой регистром положения зоны. Когда в процессе перемещения мобильный абонент переходит из зоны действия одного контроллера базовой станции в зону действия другого, то она регистрируется последним.

VLR содержит такие же данные, как и HLR, но эти данные находятся в VLR только до тех пор, пока абонент находится в зоне, контролируемой VLR. [5]

Обычно, но не обязательно, VLR связан с одним центром коммутации MSC, хотя стандарт GSM позволяет увязывать один VLR с несколькими MSC. Центр MSC представляет собой коммутационную станцию, которая выполняет все функции коммутации для мобильных станций, находящихся в области, ею обслуживаемой.

Для обеспечения услуг роуминга особенно необходимо взаимодействие между такими функциональными объектами сети сотовой связи, как VLR и HLR, которые могут быть реализованы в разном оборудовании или интегрированы, но в любом случае между ними происходит обмен данными.

Для тестирования сетевых элементов, использующих для взаимодействия между собой протокол TCAP, применяется протокол-тестер SNT-7531. В режиме симуляции протокол-тестера SNT-7531 возможна имитация одного из сетевых элементов для проверки работы другого по заранее заданным тестовым сценариям.

Пусть протокол-тестера SNT-7531 в режиме симуляции выполняет функции гостевого регистра VLR. Тогда по следующим тестовым сценариям возможна проверка функционирования подсистемы TCAP узла HLR при предоставлении услуги «роуминг».

Рассмотрим алгоритм взаимодействия элементов сети GSM при организации роуминга (рис. 4.5):

1. Прибывший мобильный абонент фиксируется ближайшей базовой станцией в гостевой сети GSM, при этом по радиointерфейсу MSC с этой базовой станцией передается его идентификатор IMSI. MSC, анализируя сообщение, полученное от мобильного абонента, узнает, что данная подвижная станция не зарегистрирована в его VLR (далее обозначается VLR1).
2. На основании международного номера абонента (IMSI) VLR1 через MSC обращается к HLR, где зарегистрирован данный абонент с заявкой на обновление данных зоны местонахождения. Для этой цели прикладная подсистема

MAP базы данных VLR1 коммутационного узла, в котором временно находится мобильный абонент, формирует и передает запрос на выполнение операции передачи информации об изменении местоположения мобильного абонента в базу данных HLR – UpdateLocation. Одновременно VLR1 запрашивает в HLR сведения о мобильном абоненте, необходимые для организации обслуживания (оговоренные подпиской виды услуг, пароли, шифры). Подсистема TCAP создает сообщение TC-BEGIN, в котором передает данный запрос. Передачей этого сообщения TCAP открывает диалог одной подсистемы MAP с другой. При этом этому диалогу присваивается идентификатор (ID=X). Далее это сообщение передается по сети посредством подсистемы SCCP.

3. Подсистема TCAP соответствующего HLR принимает и обрабатывает это сообщение, а затем передает запрос на операцию UpdateLocation подсистеме MAP.
4. HLR проверяет право абонента на роуминг. Подсистема MAP данного HLR передает подтверждение на обновление данных подсистеме TCAP, а также информацию о текущем профиле абонента в виде операции InsertSubscriberData. Далее подсистема TCAP формирует сообщение TC-CONTINUE и передает его подсистеме SCCP.
5. Транзакцию посредством посылки регистром VLR сообщения TC-END.
6. Кроме того, HLR после обновления данных обращается с заявкой к VLR (далее VLR2) через соответствующий MSC, в зоне обслуживания которого находился мобильный абонент, на отмену записи регистрации этого абонента в VLR2. Для этого подсистема MAP HLR формирует запрос на выполнение операции CancelLocation и передает ее подсистеме MAP VLR2 посредством сообщения TCAP TC-BEGIN. Таким образом, открывается новый диалог и ему присваивается идентификатор, отличный от предыдущего (ID=Y). Подсистема MAP VLR2, в свою очередь, передает в обратном направлении подтверждение о произведенных действиях, посредством сообщения TC-END, что завершает данный диалог.

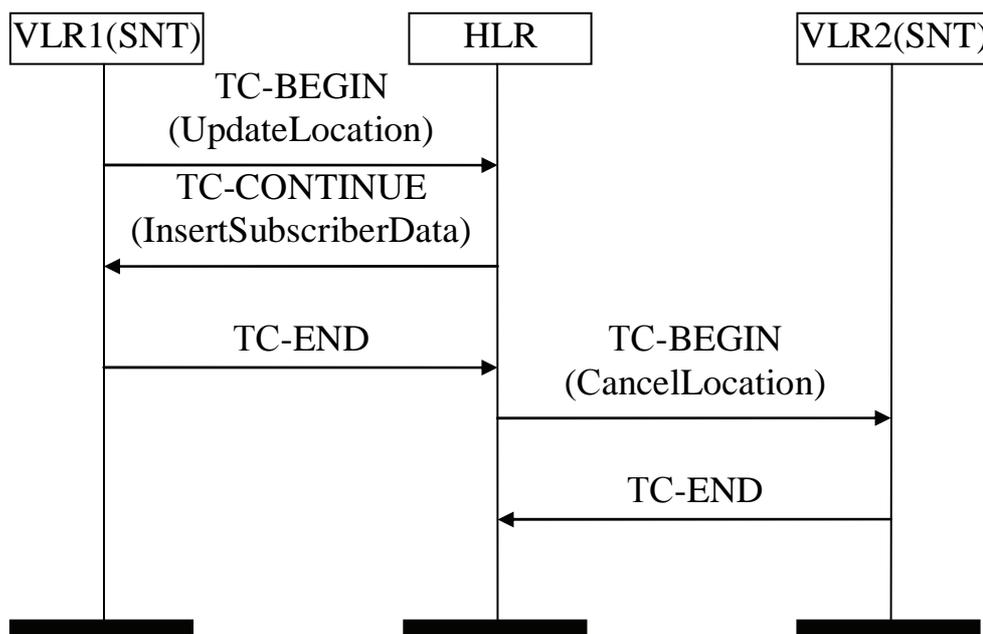


Рис. 4.5. Сценарий взаимодействия элементов сети GSM при организации роуминга (показаны только сообщения TCAP).

Рассмотрим теперь сценарий установления соединения при осуществлении входящего вызова абоненту, находящемуся в роуминге (рис. 4.6). Пусть вызывающим абонентом является абонент стационарной ТфОП:

1. Вызывающий абонент набирает номер мобильного абонента. Телефонная сеть проключает соединение до шлюзового MSC (GMSC) и передает ему номер вызываемого абонента. Шлюзовой MSC представляет собой узел, где СПС подключается к телефонным сетям с коммутацией каналов.
2. GMSC анализирует номер вызываемого абонента и передает сообщение в HLR с запросом временного роумингового номера MSRN, посылая при этом номер мобильной станции MSISDN. Для этого прикладная подсистема MAP GMSC формирует и передает запрос на выполнение операции SendRoutingInfo. Подсистема TCAP создает сообщение TC-BEGIN, в котором передает данный запрос. Передачей этого сообщения TCAP открывает диалог одной подсистемы MAP с другой, при этом этому диалогу присваивается идентификатор (ID=A). Далее это сообщение передается по сети посредством подсистемы SCCP.

3. HLR уже проинформирован о местоположении мобильного абонента. Подсистема MAP HLR принимает и анализирует запрос. На основании информации, хранящейся в HLR, осуществляется перевод номера MSISDN в международный идентификатор мобильного абонента IMSI и определяется MSC (VLR), в зоне обслуживания которого находится мобильный абонент.
4. Далее HLR запрашивает у VLR временный номер маршрутизации, для чего подсистемой TCAP открывается новый диалог, которому присваивается идентификатор ID=B, и формируется сообщение TC-BEGIN, в котором передается запрос на выполнение операции ProvideRoamingNumber.
5. Подсистема MAP VLR принимает и обрабатывает этот запрос. Если требуемая подвижная станция подключена и свободна, VLR выделяет временный роуминговый номер MSRN и ставит его в однозначное соответствие с международным идентификатором IMSI.
6. Затем VLR формирует сообщение TCAP TC-END, в котором передается выделенный номер MSRN. Этот диалог заканчивается.
7. HLR передает сообщение с временным роуминговым номером GMSC посредством подсистемы TCAP. Сообщение TC-END также завершает транзакцию.

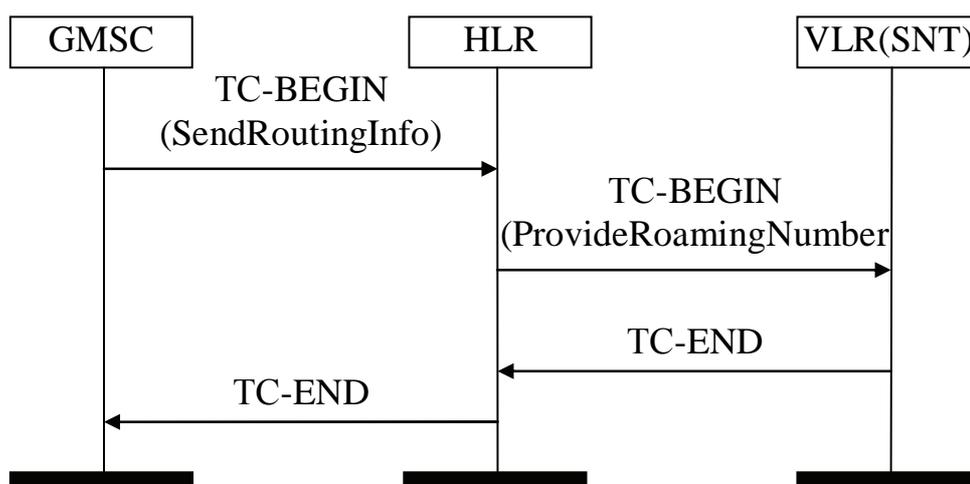


Рис. 4.6. Сценарий установления соединения при осуществлении входящего вызова абоненту, находящемуся в роуминге, от абонента ТфОП (показаны только сообщения TCAP).

8. GMSC, обладая номером MSRN, устанавливает соединение к центру коммутации MSC, в зоне обслуживания которого находится вызываемый мобильный абонент. MSC на основании номера вызываемого абонента и данных VLR определяет зону местонахождения требуемая подвижная станция. Далее MSC назначает двухсторонний пользовательский канал и передает указание подвижной станции на подключение к нему. Абоненту посылается сигнал вызова.

Далее рассмотрим сценарий организации роуминга, при котором пользователь TCAP (в данном случае имеется в виду подсистема MAP) прерывает транзакцию (рис. 4.7):

1. Прибывший мобильный абонент фиксируется ближайшей базовой станцией в гостевой сети GSM, при этом по радиointерфейсу MSC с этой базовой станцией передается его идентификатор IMSI. MSC, анализируя сообщение, полученное от мобильного абонента, узнает, что данная подвижная станция не зарегистрирована в его VLR .
2. На основании номера абонента (IMSI) VLR через MSC обращается к HLR, где зарегистрирован данный абонент с заявкой на обновление данных зоны местонахождения посредством подсистемы TCAP. Для этой цели формируется сообщение TC-BEGIN, в котором передает данный запрос на выполнение операции и передает запрос на выполнение операции UpdateLocation. В этом же сообщении VLR запрашивает в HLR сведения о мобильном абоненте, необходимые для организации обслуживания. Передачей этого сообщения TCAP открывает диалог одной подсистемы MAP с другой. Далее это сообщение передается по сети посредством подсистемы SSCP.
3. Подсистема TCAP соответствующего HLR принимает и обрабатывает это сообщение, а затем передает запрос на операцию UpdateLocation подсистеме MAP.
4. Предположим, что подсистема MAP регистра HLR решила по каким-либо причинам прервать транзакцию. Часто причиной прекращения процесса бывает несоответствие версий протокола MAP в двух одноуровневых объектах-

участниках диалога. Одна сторона, например, запрашивает старый или новый протокол, который партнер больше не поддерживает или еще не поддерживает. Тогда подсистема TCAP HLR формирует сообщение TC-U-ABORT и посылает его посредством SCCP. При этом причина прерывания может сообщаться, а может не сообщаться. В случае, если пользователю требуется передать причину прерывания, то эта информация содержится в диалоговой части сообщения.

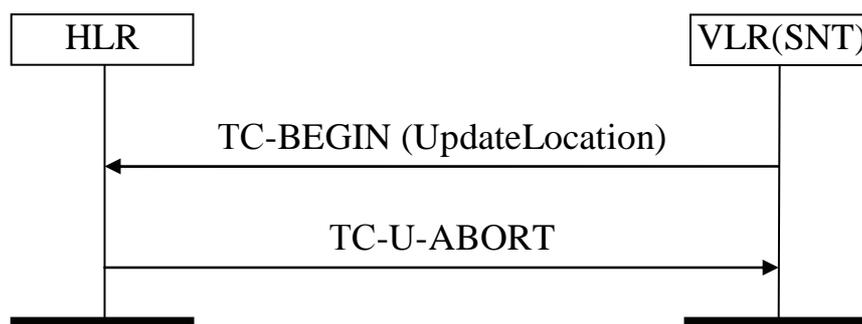


Рис. 4.7. Сценарий организации роуминга, при котором пользователь TCAP прерывает транзакцию.

#### 4.4. Анализ временных характеристик сообщений TCAP

В предыдущих параграфах были рассмотрены сценарии тестирования подсистемы TCAP, при организации предоставления услуг интеллектуальной сети (услуга «800» и телеголосование) и услуги сотовой сети стандарта GSM – роуминг.

При предоставлении интеллектуальных услуг сообщения TCAP используются для взаимодействия узла коммутации SSP и узла управления услугами SCP, содержащего базу данных, а при организации роуминга возникает необходимость использования подсистемы TCAP для взаимодействия таких элементов

сотовой сети, как HLR, VLR, EIR, которые, по сути, представляют собой базы данных, и центром коммутации MSC.

При тестировании подсистемы TCAP возникает необходимость расчета временных задержек, которые возникают в процессе транзакции, для оптимизации функционирования системы.

В звене ОКС №7 сообщения передаются с помощью пакетов, называемых сигнальными единицами. Сигнальные единицы имеют различное назначение и переменную длину. Одно сообщение может передаваться с помощью нескольких сигнальных единиц. [6]

В ОКС №7 предусматривается три типа сигнальных единиц:

1. Значащие сигнальные единицы (MSU), к которым относятся сообщения TCAP – их длина может быть до 273-х байтов.
2. Сигнальные единицы состояния звена (LSSU) используются для индикации состояния оконечных устройств и управления звеном сигнализации. Их длина может быть 7 или 8 байтов.
3. Заполняющие сигнальные единицы (FISU), которые имеют нулевую полезную длину, однако, их наличие позволяет оперативно контролировать работоспособность звена сигнализации при отсутствии пользовательского сигнального трафика. Они передаются лишь в том случае, когда отсутствуют для передачи значащие сигнальные единицы или сигнальные единицы состояния звена. [6]

При передаче в ОКС №7 сигнальные единицы состояния звена имеют наивысший приоритет. Следующий приоритет принадлежит значащим сигнальным единицам. При передаче сигнальных единиц используется дисциплина обслуживания с относительным приоритетом, т.к. нельзя прервать начатую передачу. [6]

Допустим, что сеть предоставляет  $M_y$  различных услуг (для интеллектуальной сети имеются в виду интеллектуальные услуги, например, такие как услуга «800» и телеголосование; для сотовой сети стандарта GSM, например, роуминг). Количество пользователей услуги  $u_i$ , составляет число  $N_{y_i}$ . Количество

запросов на услуги  $y_i$ , поступающее от одного пользователя в ЧНН, составляет  $\Delta_i$ . [6]

Интенсивности поступления запросов на услугу  $y_i$  в ЧНН от всех  $N_{y_i}$  пользователей рассчитываются следующим образом [6]:

$$\Lambda_i = N_{y_i} \Delta_i \quad (4.1)$$

Интенсивности поступления тех же запросов в одну секунду в течение ЧНН определяются в соответствии с [6]:

$$\lambda_i = \frac{\Lambda_i}{3600} \quad (4.2)$$

Суммарная интенсивность поступления запросов на все виды услуг, действовавших в сети, определяется согласно [6]:

$$\lambda = \sum_{i \in M_y} \lambda_i \quad (4.3)$$

Средняя интенсивность поступления запросов на услуги, приходящаяся на каждое звено ОКС рассчитывается по формуле [6]:

$$\lambda_{\text{ук}} = \frac{\lambda}{n_{\text{к}}}, \quad (4.4)$$

где  $n_{\text{к}}$  – число дуплексных звеньев ОКС, соединяющих узлы коммутации.

Вероятности появления услуг  $y_i$  определяются следующим образом [6]:

$$P_{y_i} = \frac{\lambda_i}{\lambda} \quad (4.5)$$

Среднее число транзакций на одну какую-либо услугу рассчитывается в соответствии с [6]:

$$n_{\text{тп}} = \sum_{i \in M_y} n_{\text{тп}i} P_{y_i}, \quad (4.6)$$

где  $n_{\text{тп}i}$  – число транзакций, обеспечивающих реализацию услуги  $y_i$ .

Значения  $n_{\text{тп}i}$  обычно задаются в исходных данных, исходя из имеющейся статистики [6].

Часть услуг требует для своего выполнения передачи некоторых статистических данных. Обозначим через  $S_i$ , процент каждой из услуг  $y_i$ , требующий передачи дополнительной статистической информации. Среднее число тран-

закций на одну услугу, с учетом необходимой передачи статистики определяется согласно [6]:

$$n_{\text{TPS}} = \sum_{i \in N_y} \frac{n_{\text{TPi}} P_{yi} S_i}{100} + n_{\text{TP}} \quad (4.7)$$

Среднее число транзакций, осуществляемых в одну секунду, с учетом передачи статистических данных рассчитывается следующим образом [6]:

$$\lambda_{\text{TP}} = n_{\text{TPS}} \lambda \quad (4.8)$$

Указанная интенсивность осуществления транзакций служит основой для расчета требуемого числа звеньев системы ОКС №7 между узлами коммутации [6].

Допустим, что каждая транзакция включает в себя  $n_{\text{ЗН}}$  значащих сигнальных единиц, передаваемых в одном направлении по звену ОКС. Средняя длительность группы значащих сигнальных единиц, передаваемой в одном направлении в течение одной транзакции, рассчитывается по формуле [6]:

$$\tau_{\text{TP}} = n_{\text{ЗН}} \tau_{\text{ЗН}}, \quad (4.9)$$

где  $\tau_{\text{ЗН}}$  – средняя длительность значащей сигнальной единицы.

Обозначим через  $\beta_{\text{TP}}$  – среднюю длину пакета, передаваемого в течение одной транзакции в одном направлении канала ОКС №7, а через  $\beta_{\text{ЗН}}$  – среднюю длину значащей сигнальной единицы, выраженные в байтах. Количество  $n_{\text{ЗН}}$  значащих единиц, передаваемых в одном направлении в течение одной транзакции определяется в соответствии с [6]:

$$n_{\text{ЗН}} = \frac{\beta_{\text{TP}}}{\beta_{\text{ЗН}}} \quad (4.10)$$

Значения  $\beta_{\text{TP}}$  и  $\beta_{\text{ЗН}}$  обычно задаются в пределах 140 и 53 байта соответственно, исходя из имеющихся статистических данных. Следовательно, каждая транзакция осуществляет передачу в одном направлении, в среднем, 2,6 сигнальной единицы. [6]

Помимо значащих единиц в канале присутствует поток сигнальных единиц состояния звена с интенсивностью  $\lambda_{\text{СЗ}}$ , практически не зависящей от посту-

пающих запросов на выполнение услуг, и средним временем передачи  $\tau_{\text{СЗ}}$ . Наконец, всё оставшееся свободное время в канале заполняется потоком заполняющих сигнальных единиц, с интенсивностью  $\lambda_{\text{ЗП}}$  и длительностью передачи  $\tau_{\text{ЗП}}$ . [6]

Длительности передачи сигнальных единиц зависят от их длины и скорости передачи информации в канале  $V_{\text{К}}$  [6].

Если обозначить  $\beta_{\text{ЗН}}$ ,  $\beta_{\text{СЗ}}$  и  $\beta_{\text{ЗП}}$  соответствующие средние длины сигнальных единиц, выраженные в байтах, то соответствующие длительности передачи рассчитываются следующим образом [6]:

$$\tau_{\text{ЗН}} = \frac{8 \cdot \beta_{\text{ЗН}}}{V_{\text{К}}} \quad (4.11)$$

$$\tau_{\text{СЗ}} = \frac{8 \cdot \beta_{\text{СЗ}}}{V_{\text{К}}} \quad (4.12)$$

$$\tau_{\text{ЗП}} = \frac{8 \cdot \beta_{\text{ЗП}}}{V_{\text{К}}} \quad (4.13)$$

Обычно скорость модуляции  $V_{\text{К}}$  в канале ОКС №7 составляет 64 кбит/с. Если принять значения длин сигнальных единиц, соответственно:  $\beta_{\text{ЗН}} = 53$  байтов,  $\beta_{\text{СЗ}} = 8$  байтов,  $\beta_{\text{ЗП}} = 6$  байтов, то получим следующие значения средних времен передачи сигнальных единиц [6]:

$$\tau_{\text{ЗН}} = \frac{8 \cdot 53}{64000} = 6,62 \cdot 10^{-3} \text{ с} = 6,62 \text{ мс}$$

$$\tau_{\text{СЗ}} = \frac{8 \cdot 8}{64000} = 1 \cdot 10^{-3} \text{ с} = 1 \text{ мс}$$

$$\tau_{\text{ЗП}} = \frac{8 \cdot 6}{64000} = 0,75 \cdot 10^{-3} \text{ с} = 0,75 \text{ мс}$$

Если принять среднее число значащих единиц передаваемых в течение одной транзакции по каналу ОКС в одну сторону  $n_{\text{ЗН}} = 2,6$ , то среднее время передачи одной транзакции рассчитывается следующим образом [6]:

$$\tau_{\text{ТР}} = n_{\text{ЗН}} \tau_{\text{ЗН}} = 6,62 \cdot 2,6 = 17,2 \text{ мс}$$

Количество звеньев ОКС №7 между узлами коммутации  $n_k$  определяется исходя из требования минимальной загрузки канала  $\rho_{\text{ОКС}}$ , значение которой выбирается в пределах  $\rho_{\text{ОКС}} = 0,2$  [6]:

$$n_k = \frac{\lambda_{\text{ТР}} \tau_{\text{ТР}}}{\rho_{\text{ОКС}}} \quad (4.14)$$

Значение  $n_k$  округляется до ближайшего большего целого числа [6].

Интенсивность поступления транзакций в расчете на одно звено ОКС №7 является одной из основных характеристик работоспособности звена и рассчитывается по формуле [6]:

$$\lambda_{\text{ТРК}} = \frac{\lambda_{\text{ТР}}}{n_k} \quad (4.15)$$

Предположим, что поступающие транзакции, а также сигнальные единицы состояния звена и заполняющие сигнальные единицы образуют простейшие пуассоновские потоки. На самом деле это не так. Однако принятие экспоненциального распределения обеспечивает некоторый дополнительный запас при расчетах. [6]

Простейшая модель канала передачи данных между узлами коммутации представляет собой одноканальную СМО, в которой обрабатываются три потока сообщений:

$Z_1$  – поток сигнальные единицы состояния звена, имеющих наивысший приоритет;

$Z_2$  – поток транзакций, реализующих запросы на предоставление услуг;

$Z_3$  – поток заполняющие сигнальные единицы, имеющих самый низший приоритет. [6]

Коэффициент загрузки канала сигнальными единицами состояния звена, образующими поток  $Z_1$ , рассчитывается следующим образом [6]:

$$\rho_1 = \lambda_{\text{СЗ}} \tau_{\text{СЗ}} \quad (4.16)$$

Коэффициент загрузки канала значащими сигнальными единицами, образующими поток  $Z_2$ , рассчитывается согласно [6]:

$$\rho_2 = \lambda_{\text{ТРК}} \tau_{\text{ТР}} \quad (4.17)$$

Поскольку всё время канала, не занятое передачей транзакций и сигнальных единиц состояния звена, используется для передачи заполняющих единиц, а суммарный коэффициент загрузки канала всегда равен 1, коэффициент загрузки канала заполняющими сигнальными единицами, образующими поток  $Z_3$  определяется по формуле [6]:

$$\rho_3 = 1 - (\rho_1 + \rho_2) \quad (4.18)$$

Заявки, поступившие в канал и ожидающие передачи, заносятся в соответствующие очереди  $O_1$ ,  $O_2$  и  $O_3$ . В очередях заявки упорядочены по времени их поступления. Когда в канале заканчивается передача очередного сообщения, то управление переходит к программе «диспетчер», которая выбирает для очередной передачи сообщение с наивысшим приоритетом, если очереди более старших приоритетов не содержат сообщений (т.е. оказываются пустыми). Выбранное для передачи сообщение захватывает канал на все время его передачи. Если в систему поступает  $N$  простейших потоков сообщений с интенсивностями  $\lambda_1, \dots, \lambda_N$ , средние длительности передачи сообщений каждого типа, соответственно, равны  $\tau_1, \dots, \tau_N$ , и вторые начальные моменты соответственно  $\tau_1^{(2)}, \dots, \tau_N^{(2)}$ , то среднее время  $t_K$  ожидания в очереди сообщений, имеющих приоритет  $K$ , определится соотношением [6]:

$$t_K = \frac{\sum_{i=1}^N \lambda_i \tau_i^{(2)}}{2(1 - R_{K-1})(1 - R_K)}, \quad (4.19)$$

где  $R_{K-1} = \rho_1 + \rho_2 + \dots + \rho_{K-1}$ ;

$R_K = \rho_1 + \rho_2 + \dots + \rho_K$ ;

$\rho_i$  – загрузки, создаваемые сигнальной единицей  $i$ -го типа.

Рассчитаем коэффициента вариации длины сообщений согласно [6]:

$$v_i = \frac{\sigma_i}{\tau_i}, \quad (4.20)$$

где  $\sigma_i$  – среднеквадратическое отклонение времен передачи сообщений  $i$ -го типа.

Используя формулу (4.19), преобразуем выражение (4.20) следующим образом:

$$t_k = \frac{\sum_{i=1}^N \rho_i \tau_i (1 + v_i^2)}{2 (1 - R_{k-1})(1 - R_k)} \quad (4.21)$$

В рассматриваемом конкретном случае анализа имеются всего  $N=3$  типа передаваемых сообщений [6].

Согласно [6], для сообщений потока  $Z_1$  ( $K=1$ ):

$$R_1 = \rho_1, \tau_1 = \tau_{C3}, v_1 = v_{C3};$$

для сообщений потока  $Z_2$  ( $K=2$ ):

$$R_2 = \rho_1 + \rho_2, R_1 = \rho_1, \tau_2 = \tau_{TP}, v_2 = v_{TP};$$

для сообщений потока  $Z_3$  ( $K=3$ ):

$$R_3 = \rho_1 + \rho_2 + \rho_3 = 1,$$

$$R_2 = \rho_1 + \rho_2, \tau_3 = \tau_{3П}, v_3 = v_{3П},$$

где  $v_{C3}$ ,  $v_{TP}$ ,  $v_{3П}$  – коэффициенты вариации длин сообщений для потоков сигнальных сообщений состояния звена, транзакций и заполняющих сигнальных единиц соответственно.

При определении значений коэффициентов вариации длин сообщений необходимо учесть, что сигнальные единицы состояния звена и заполняющие единицы имеют практически постоянную длину ( $\sigma_{C3}=0$ ,  $\sigma_{3П}=0$ ) и, следовательно,  $v_{C3}=0$  и  $v_{3П}=0$  [6].

Сообщения транзакций, напротив, имеют информационные части переменной длины. Если предположить, что длины указанных сообщений распределены по экспоненциальному закону, то  $\sigma_{TP} = \tau_{TP}$ , и коэффициент вариаций  $v_{TP}$  оказывается равным 1. [6]

Учитывая все сказанное, определим значения времени ожидания в очередях для сообщений каждого типа. [6]

Среднее время ожидания в очереди на передачу для сигнальных единиц состояния звена, имеющих наивысший приоритет определяется следующим образом [6]:

$$t_{\text{сзо}} = \frac{\rho_1 \tau_{\text{сз}} + 2 \rho_2 \tau_{\text{тр}} + \rho_3 \tau_{\text{зп}}}{2 (1 - R_1)} \quad (4.22)$$

Среднее время ожидания в очереди на передачу для сообщений транзакций, имеющих второй приоритет, рассчитывается согласно [6]:

$$t_{\text{тро}} = \frac{\rho_1 \tau_{\text{сз}} + 2 \rho_2 \tau_{\text{тр}} + \rho_3 \tau_{\text{зп}}}{2 (1 - R_1)(1 - R_2)} \quad (4.23)$$

Среднее время ожидания в очереди на передачу для заполняющих сообщений оказывается бесконечно большим, т.к. очередь этих сообщений считается неограниченной, поскольку значение  $R_3=1$ , и определяется по формуле [6]:

$$t_{\text{зпо}} = \frac{\rho_1 \tau_{\text{сз}} + 2 \rho_2 \tau_{\text{тр}} + \rho_3 \tau_{\text{зп}}}{2 (1 - R_1)(1 - R_2)(1 - R_3)} \quad (4.24)$$

Так как в работе рассматриваются тестовые сценарии подсистемы ТСАР, то для нас интерес представляют только временные задержки в очередях передаваемых транзакций  $t_{\text{тро}}$ . Среднее время передачи и ожидания в очередях для одного сообщения ТСАР составляет:

$$t_{\text{тр}} = t_{\text{тро}} + \tau_{\text{тр}} \quad (4.25)$$

При предоставлении какой-либо услуги происходит обмен сообщениями ТСАР между соответствующими сетевыми элементами. Временная задержка при осуществлении диалога ТСАР обусловлена, кроме задержек, связанных с передачей сообщений ТСАР, задержками при обработке запросов этими сетевыми элементами.

Например, рассмотрим, из чего складывается временная задержка при осуществлении диалога ТСАР для предоставления услуги «800» (п.4.1, рис. 4.1). Взаимодействие SSP и SCP начинается с момента поступления на станцию, содержащую SSP, последней цифры набора кода и номера услуги. SSP осуществляет анализ полученной информации, инициирует запрос услуги передает его посредством протокола ТСАР в виде сообщения TC-BEGIN по каналу ОКС №7. Сообщение, полученное SCP, анализируется, обрабатывается компьютерами, в результате чего SSP получает ответ из SCP, в котором содержится информация о том, как произвести услугу, в виде сообщения TC-CONTINUE.

После получения указанной информации, SSP сообщением TC-END информирует SCP об окончании обмена.

Таким образом, в данном случае временная задержка складывается из следующего:

$$T_{\text{TCAP}} = 3 t_{\text{TP}} + 2 t_{\text{SSP}} + 2 t_{\text{SCP}}$$

где  $t_{\text{SSP}}$  – среднее время, затрачиваемое SSP на обработку одного запроса; (4.26)

$t_{\text{SCP}}$  – среднее время, затрачиваемое SCP на обработку одного запроса.

Но, т.к. после того как в сообщении TC-CONTINUE узлу коммутации SSP были доставлены все необходимые сведения для продолжения установления соединения, задержка функционирования интеллектуальной сети, вносимая передачей сообщений TCAP определяется следующим образом:

$$T_{\text{INAP}} = 2 t_{\text{TP}} + t_{\text{SSP}} + t_{\text{SCP}} \quad (4.26)$$

Выводы по главе. Для предоставления своих услуг возможностями TCAP пользуются такие сети, как интеллектуальная сеть и сотовая сеть подвижной связи стандарта GSM. В этой главе были рассмотрены некоторые тестовые сценарии подсистема TCAP при организации предоставления таких услуг, как услуга «800», телеголосование и роуминг. В соответствии с этими сценариями возможно проведение тестирования TCAP. Для этого вместо одного из сетевых элементов подключают тестер в режиме симуляции (например, протокол-тестер SNT-7531), который содержит набор подобных тестовых сценариев, по которым осуществляется проверка функционирования системы. Также был проведен анализ временных характеристик TCAP и показан расчет задержек, которые вносятся сообщениями TCAP, при предоставлении какой-либо услуги. Эти временные задержки связаны с задержками при передаче сообщений TCAP, а также задержками при обработке запросов этими сетевыми элементами.

## Заключение

В работе показана роль стека протоколов ОКС №7 для современных сетей связи, а также место подсистемы ТСАР в ней. Сегодня, когда прослеживается тенденция отделения функций коммутации от функций управления услугами, возникает необходимость обмена данными между распределенными внутрисетевыми ресурсами для предоставления пользователю различных услуг. Для этого используются возможности подсистемы ТСАР. Поскольку спрос на подобные услуги сейчас все возрастает, использование подсистем ТСАР становится все более и более необходимым. Но, несмотря на все возрастающее практическое использование протокола ТСАР, его описание в отечественных источниках встречается относительно редко.

В работе исследованы два аспекта проектирования сетей с ТСАР:

- тестирование подсистемы ТСАР. Для этого были разработаны тестовые сценарии обмена сообщениями между подсистемами ТСАР сетевых узлов при предоставлении некоторых услуг интеллектуальной и сотовой сетей. Выполняя эти тесты при испытании реальных сетей связи, пользователь может проверить функциональные возможности подсистемы ТСАР;
- расчет задержек сообщений ТСАР. В работе также представлена модель расчета временных задержек сообщений ТСАР. При наличии соответствующих статистических данных эта модель позволяет рассчитать средние временные задержки, вносимые сообщениями ТСАР, для каждой сети.

Таким образом, что цель исследования реализована, а поставленные для ее достижения задачи выполнены.

## Список литературы

1. Аджемов А.С., Кучерявый А.Е. Система сигнализации ОКС №7. – М.: Радио и связь, 2002.
2. Гольдштейн Б.С. Сигнализация в сетях связи. Том 1. – 4-е изд. – СПб: БХВ-Санкт-Петербург, 2005.
3. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. – М.: Радио и связь, 2000.
4. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Стек протоколов ОКС7. Подсистема МТР. – М.: Радио и связь, 2003.
5. Карташевский В.Г., Семенов С.Н., Фирстова Т.В. Сети подвижной связи. – М.: Эко-Трендз, 2001.
6. Лихтциндер Б.Я., Кузякин М.А., Росляков А.В., Фомичев С.М. Интеллектуальные сети связи. – М.: Эко-Трендз, 2002.
7. Попов В.И. Основы сотовой связи стандарта GSM. – М.: Эко-Трендз, 2005 г.
8. Росляков А.В. Общеканальная система сигнализации №7. – 2-е изд., испр. – М.: Эко-трендз, 2002. (Инженерная энциклопедия «Технологии электронных коммуникаций»).
9. Dreher R., Harte L., Beninger T. SS7 Basic. 2<sup>nd</sup> Edition. – 2002.
10. Heine G. GSM Network: Protocols, Terminology and Implementation. – Hardcover, 1999.
11. <http://niits.ru/products/?test-snt7531>.
12. ITU-T Recommendation Q.771: Specifications of Signalling System No. 7 – Transaction capabilities application part. Functional description of transaction capabilities.
13. ITU-T Recommendation Q.772: Specifications of Signalling System No. 7 – Transaction capabilities application part. Transaction capabilities information element definitions.

14. ITU-T Recommendation Q.773: Specifications of Signalling System No. 7 – Transaction capabilities application part. Transaction capabilities formats and encoding.
15. ITU-T Recommendation Q.787: Specifications of Signalling System No. 7 – Test specification. Transaction capabilities test specification.
16. ITU-T Recommendation Z.120: Criteria for the use and applicability of formal Description Techniques. Message Sequence Chart.

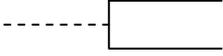
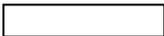
## Рекомендации МСЭ по вопросам ОКС №7

Описание подсистем, функций, компонентов	Рекомендации МСЭ
Введение в ОКС №7	Q.700
Подсистема MTP	Q.701-Q.704, Q.706, Q.707
Структура сети сигнализации ОКС №7	Q.705
Подсистема SCCP	Q.711-Q.714, Q.716
Подсистема TUP	Q.721-Q.725
Дополнительные услуги	Q.730-Q.737
Подсистема OMAP	Q.750, Q.752-Q.755
Подсистема ISUP	Q.761-Q.764, Q.766, Q.767
Подсистема TCAP	Q.771-Q.775
Тестирование MTP, TUP, ISUP, SCCP, TCAP	Q.780-Q.787
Подсистема MAP	Q.1051
Подсистема INAP	Q.1205, Q.1208, Q.1211, Q.1213-Q.1215, Q.1218, Q.1219, Q.1290
Соответствие ОКС №7 и модели взаимодействия открытых систем OSI	Q.1400

## Рекомендации МСЭ по подсистеме средств транзакции

Рекомендация МСЭ	Раздел рекомендации	Содержание рекомендации
Q.771	Q.771.1 Q.771.2 Q.771.3	Функциональное описание возможностей транзакции. Введение. Обзор. Услуги, предоставляемые транзакцией, основанной на сетевой услуге, не ориентированной на соединение.
Q.772	Q.772.1 Q.772.2 Q.772.3 Q.772.4	Определение информационных элементов возможностей транзакции. Общие положения. Порция транзакции. Порция компоненты. Порция диалога.
Q.773	Q.773.1 Q.773.2 Q.773.3 Q.773.4	Форматы возможностей транзакции и кодирования. Введение. Соглашение о формальном описании. Описание абстрактного синтаксиса. Представление сообщения.
Q.774	Q.774.1 Q.774.2 Q.774.3	Процедуры возможностей транзакции. Введение. Адресация. Возможности транзакции, основанные на услугах сети, не ориентированных на соединение

## Основные символы, используемые в MSC

Название	Символ	Название	Символ
Комментарий		Цикл	
Заголовок требований		Конец требований	
Основная ось требований 1		Основная ось требований 2	
Сообщение		Условие	
Запуск таймера (1 вар.)		Запуск таймера (2 вар.)	
Перезапуск таймера		Сброс таймера (1 вар.)	
Сброс таймера (2 вар.)		Завершение таймера (1 вар.)	
Завершение таймера (2 вар.)		Завершение таймера (3 вар.)	
Создание		Остановка	
Разделить			